VA Mobile Infrastructure Services

VA MIS Disaster Recovery Plan

# Introduction

## Disaster Recovery Approach

Booz Allen will work in conjunction with Verizon Terre mark to provide an array of Disaster Recovery (DR) and Virtual Disaster Recovery (VDR) services to include DR testing and failover during an actual disaster incident. If a disaster incident occurs, we will work with the VA PM to determine if there is a need to failover (depending on the estimated recovery time at the primary site). If the impacted VA MIS programs must failover, we will create a contingency team that will immediately start to bring up the secondary site in Miami, FL. Once the site is up, we will work with application owners to validate application functionality and then request VA to crossover to the secondary site.

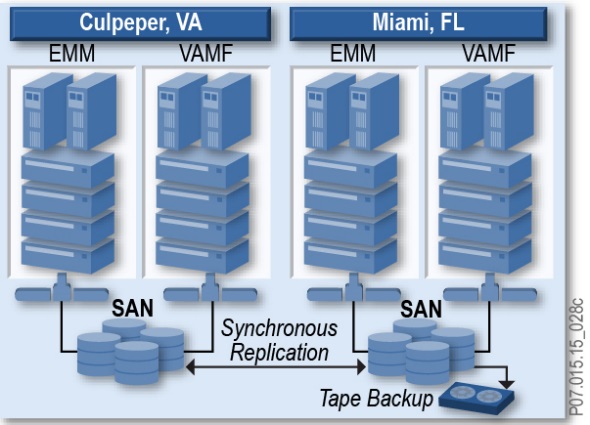
The Booz Allen Team will provide an IaaS/PaaS solution that supports DR using the Culpeper and Miami data centers that already house VA Dedicated Private Cloud services. The Culpeper and Miami data centers, located within the continental United States and authorized to host U.S. government systems, have cloud services that can operate completely independently of the other, thereby enabling flexibility for the VA. The two data centers conform to the disaster recovery guidance in VA Handbook 6500.8. Further, both Culpeper and Miami data centers have dedicated connectivity to VA Business Partner Extranet (BPE). The Terre mark Culpeper data center will continue to be utilized as the primary cloud location with the Terre mark Miami data center operating as the failover site.

Figure 1: Disaster Recovery Centers

The Booz Allen Team proposes that Virtual Disaster Recovery (VDR) services be utilized for VA EMM, VAMF, and associated environments. This will provide a hot-warm DR capability to maximize uptime, minimize data loss, and reduce downtime of applications. In the event that the primary site for the EMM and/or VAMF enclave(s) experiences a critical outage, the secondary site shall be up and running in no later than 3 hours once the decision from the VA PM has been made. Mobile App Environment (MAE) and Enterprise Cloud Environment (ECE) enclaves are only configured for the hot-cold capability, with no established Recovery Time Objective (RTO) identified at this time. In order to maintain data consistency across multiple sites, we will utilize current SAN replication technologies to replicate data from the primary site to the secondary site. Once replicated to the secondary data center, all data will be backed up to tape using the approach provided in the next section and retained in accordance with VA 6500 guidelines for systems that can contain PII/PHI.

The virtual disaster and recovery from the disaster testing is in accordance with the VA Handbook 6500.8 and will migrate the VA MIS cloud and enclaves to the secondary site to test the complete disaster recovery system. Following the disaster recovery test, the Booz Allen Team will provide a DR after Action Report (AAR) within ten days of completion of testing, which will include lessons learned and the identification of gaps in the current DR Plan. Our “communicate early, communicate often” approach should minimize the risk of any surprises during Disaster Recovery Testing. Our team assumes VA will exercise its right to conduct independent, hands-on testing with representatives from the team present before considering the results acceptable. Our subject matter experts (SMEs) will prepare role-specific zero-knowledge usage guides for the end-user roles. When a disaster recovery scenario occurs, it will be given a priority over other VA requests. The Booz Allen Team will provide an IaaS/PaaS solution that supports DR using the Culpeper and Miami data centers that already house VA Dedicated Private Cloud services. The Culpeper and Miami data centers, located within the continental United States and authorized to host U.S. government systems, have cloud services that can operate completely independent of the other enabling flexibility for the VA. The two data centers conform to the disaster recovery guidance in the VA Handbook 6500.8. Further, both Culpeper and Miami data centers have dedicated connectivity to the VA Business Partner Extranet (BPE). The Verizon Terre mark Culpeper data center will continue to be utilized as the primary cloud location with the Verizon Terre mark Miami data center operating as the failover site.

Disaster Recovery relies upon data consistency across multiple cloud environments and the ability to direct network traffic to the healthiest cloud. The DR administration and testing will be performed by the Booz Allen Team utilizing Verizon Terre mark’s orchestration tool, Infinicenter or through RESTful v4 APIs. During a DR event, the Booz Allen Team, working in conjunction with our VA NSOC counterparts will be able to fail an environment from the primary site to the secondary site. The Team will also coordinate with the VA NSOC to redirect traffic from the primary site to the secondary site and will coordinate any necessary Domain Name System (DNS) changes. Once the DR event is over, the Booz Allen Team can use Infinicenter to return operations back to the primary site again while coordinating with the VA NSOC to redirect traffic back to the primary site. The Booz Allen Team will also perform a full failover to the secondary site when requested from VA and document all results in an after action report for approval by the VA PM/COR. Please note that the DR and VDR steps captured in this document follow the standard operating procedures that Verizon Terre mark conducts and aligns closely with the documentation currently maintained by Verizon (document artifact: DR Failover VDR Exercise and Configuration Overview v09142015.pdf)

## Backup and Recovery Approach

A proven backup and recovery process provides organizations with the confidence and ability to restore applications and data with minimal level of effort, minimizing potential downtimes and impact to users. The Booz Allen Team’s IaaS/PaaS solution includes a tiered backup and recovery approach and compliant with Federal and VA System of Record (SOR) policies. All data will be copied from the Culpeper SAN to the Miami SAN to allow for DR services and backup to encrypted tape drives. VA data will be archived offsite in Miami by the Booz Allen Team for the period of the contract. The Booz Allen Team understands that HIPAA PII and PHI must be retained for seven (7) years as specified in the VA Handbook 6500 and NIST 800-5, Revision 4. Upon the expiration of the contract, the Booz Allen Team will work with the VA to properly deliver stored VA data. Should the VA require the Booz Allen/Verizon Terre mark Team to hold data beyond the contract terms, the Parties will negotiate to come to mutual agreement for any additional support required, any associated costs, and any additional applicable terms and conditions.

The Booz Allen Team will provide the ability to back up and restore VA data, including all tools and dashboards, through SAN replication and tape backup. The backups can be tested by restoring the backup on another server and validating application functionality. The Booz Allen Team will support hypervisor snapshots per the VM State Saving Frequency and Retention table provided in the PWS. Full system state snapshots are configured through the cloud management tools, which allow users with appropriate permissions to create and delete snapshots for the selected virtual machine. The Booz Allen Team will also work with VA to set aside a window in which snapshots can be tested and then restored to ensure expected operation. Ad-hoc requests for restoration of snapshots will align with current workflows and processes that exist in the VA. The backups will be stored online and the tapes will be shipped offsite to a facility for storage. Finally, all **backup and recovery** logs will be provided to VA when requested.

# Duration of Plan

The *VAMIS DR Plan* will remain in effect until termination of VAMIS as directed by VA (or other authorities) or at the time when turnover of residual program responsibilities to appropriate organizations is complete.

# Authorities and References

The *VAMIS DR Plan* is based upon regulations, documentation, and guidance from VA and other federal authorities involved with DR planning and management, including:

* DCID6/3 (June 5, 1999), *Protecting Sensitive Compartmented Information Within Information Systems*
* VA Handbook 6500, *Information Security Handbook*
* OMB Circular A-130 (February 1996), *Management of Federal Information Resources*
* Presidential Decision Directive 67 (October 1998), *Enduring Constitutional Government and Continuity of Government Operations*
* Executive Order 12656 (November 1988), *Assignment of Emergency Preparedness Responsibilities*
* Federal Information Processing Standards (FIPS) Publication 87 (March 1981), *Guidelines for Automated Data Processing (ADP) COOP/DR Planning*

# Plan Objectives

A disaster can result from a number of accidental, malicious, or environmental events such as fire, flood, terrorist attack, human error, and software or hardware failures. For the purposes of the *VAMIS DR Plan,* a disaster is defined as an incident which results in the loss of computer processing at the private cloud deployed at the Verizon Terre mark facility in Culpeper, VA.

The primary objective of the *VAMIS DR Plan* is to ensure the continued operation of identified business critical systems in the event of a disaster.

Specific goals of the plan are:

* To be operational at a standby facility within eight (8) hours as defined in the Service Level Agreement (SLA) with the hosting provider (Verizon Terre mark), providing that VA makes changes to their Domain Naming Service (DNS) records to complete the migration. If not, service will be degraded until VA completes the process to make the required DNS changes.

**Note**: The hosting provider (Verizon Terre mark) leadership is responsible for initiating the DNS request to VA Network and Security Operations Center (NSOC).

* To operate at a standby facility indefinitely or until the primary facility is brought back online. (The goal is to return to operations at the primary site as soon as possible to prevent a degraded state of capability. While in Miami, FL, VAMIS cloud enclave environments are unable to service any customer requests for expansion of services on the Platform as a Service (PAAS) offering.)
* To reinstate Verizon Terre mark facilities in Culpeper, VA, as soon as is reasonably possible after repairs are completed from the disaster.
* To minimize the disruption to the private clouds deployed at Verizon Terre mark in Culpeper, VA.

# Plan Assumptions

The following assumptions are made:

* Human safety is the first priority of the *VAMIS DR Plan*. At no time will personnel be requested to be in physical danger for the sake of maintaining operations, or protecting equipment or government property.
* Both geographical locations (Culpeper, VA, and Miami, FL,) will not be affected by an event simultaneously.
* This plan covers the VAMIS enclave environments infrastructure which include:
* Federal and Private Clouds deployed at Verizon Terre mark in Culpeper, VA, and Miami, FL
* Interconnections and interfaces with VA data centers and external   
  information sources
* All essential equipment and devices with redundant counterparts at the DR site will automatically fail-over in the event of a primary equipment or device failure.
* Terre mark will follow and activate their own DR activities for reporting events specific to, or potentially affecting, the VAMIS enclave environments.
* VAMIS enclave Environments cannot be moved or replicated to another site or environment without the explicit consent of VA.
* Drills and exercises will be held to train employees and reinforce disaster preparedness procedures. These exercises include the Virtual DR exercises and a full DR exercises.

# Disaster Management Team Charter

The Disaster Management team is responsible for the following actions:

* Making decisions about restoring the computer processing environment to provide the identified level of service to users
* Managing all the recovery teams and liaising with Verizon Terre mark management, VA senior management and stakeholders, and users, as appropriate
* Maintaining audit and security controls during the recovery from disaster
* Controlling and recording emergency costs and expenditures

## Responsibilities

The Disaster Management team will perform the following activities in support of the actions listed in Section 6:

* Evaluating the extent of the problem and potential consequences
* Notifying senior management of the disaster, recovery progress and problems
* Initiating DR procedures
* Co-coordinating recovery operations
* Monitoring recovery operations and ensuring the schedules are met
* Documenting recovery operations
* Liaising with the VA senior management and stakeholders
* Recording emergency extraordinary costs and expenditures
* Making a detailed accounting of damages to aid in insurance claims
* Ensuring the conversion to the standby facilities and the final resumption of operations at the data center are under sufficient audit control to provide reliability and consistency to the accounting records
* Monitoring for adherence to computer security standards
* Ensuring appropriate arrangements are made to restore the site and return to the status quo within the time limits allowed for emergency mode processing
* Approving the results of audit tests on the applications which are processed at the standby facility shortly after they have been produced
* Declaring that the DR Plan is no longer in effect when computer processing is restored at the primary site

# Cloud Enclave Operations Team Charter

The VAMIS cloud enclave environments are actively monitored by Verizon Terre mark. The cloud enclave team is composed of members of the VAMIS cloud enclave support team and Verizon Terre mark who perform different but essential functions to sustain communication, connectivity, and availability of a standby site.

The cloud enclave team is responsible for the following:

* Ensuring the standby equipment meets the recovery schedules
* Installing the computer hardware and setting up operating systems at the standby facility
* Obtaining all appropriate historical and current data from the vault location and restoring an up to date application systems environment
* Providing the appropriate management and staffing of the standby computer processing center, data control, Help Desk and media control/tape library to meet the defined level of user requirements
* Supporting operable versions of all critical applications needed to satisfy the minimum operating requirements
* Performing backup activities at the standby site

## Responsibilities

Within Verizon Terre mark there are follow responsibilities:

* Providing ongoing technical support at the standby facility
* Working with the Networks team to restore local and wide area data communications services to meet the minimum processing requirements
* Obtaining all necessary backups from off-site storage
* Initiating operations at the standby facility
* Providing sufficient personnel to support operations at the standby facility
* Re-establishing the Help Desk, and data control and media control/tape library functions at the standby facilities
* Managing the standby facilities to meet users’ requirements
* Arranging for acquisition and/or availability of necessary computer supplies
* Ensuring all documentation for standards, operations, vital records maintenance, application programs etc. are stored in a secure/safe environment and reassembled at the standby facilities, as appropriate

Within the VAMIS Cloud Enclave Environments there are follow responsibilities:

* Re-establishing software libraries and databases to the last good backup
* Co-coordinating the user groups to aid the recovery of any non-recoverable (i.e., not available on the latest media tape dump) data
* Establishing processing schedule and informing user contacts
* Providing ongoing technical support at the standby facility
* Re-establishing and setting up the VMs and latest version of the operating system at the standby facility

# Networks Team Charter

The Networks team is responsible for all computer networking and communications, including arranging new local and wide area data communications facilities and a communications network to link the standby facility to the critical users.

## Responsibilities

The Networks team has the following responsibilities:

* Evaluating the extent of damage to the voice and data network and discussing alternate communications arrangements with telecom service providers
* Defining the priorities for restoring the network in the user areas
* Ordering the voice and data communications and equipment as required
* Supervising the line and equipment installation for the new network
* Providing necessary network documentation
* Providing ongoing support of the networks at the standby facility
* Re-establishing the networks at the primary site when the post disaster restoration is complete

# Facilities Team Charter

The Facilities team is responsible for the general environment including buildings, services and all environmental issues outside of the computer rooms. This team has responsibility for security, health and safety and for procuring alternative building facilities, including:

* Arranging for an alternate or standby facility
* Controlling security at the standby facility and the damaged site

**Note:** physical security may need to be increased.

## Responsibilities

The Facilities team has the following responsibilities:

* Working with the Networks team to have lines ready for rapid activation
* As soon as the standby site is occupied, cleaning up the disaster site and securing that site to prevent further damage

# Communications Team Charter

The Communications team is responsible for obtaining communications directives from the Disaster Management team, and communicating information during the disaster and restoration phases to employees and the VA (e.g., press, television, radio).

## Responsibilities

The Communications team has the following responsibilities:

* Liaising with the VAMIS cloud enclave support team, VA, and Verizon Terre mark to obtain directives on the messages to communicate
* Informing VA management and project teams of any potential delays
* Informing employees of the recovery progress of the schedules
* Ensuring there are no miscommunications that could damage the image of the company
* Any other public relations

# Recovery Procedures

The Verizon Terre mark DR procedures will continue to be executed for the existing VA cloud enclaves. All details for DR contained within the subsections below align with operating procedures currently in place at Verizon Terre mark and will be executed accordingly during scheduled and unscheduled disaster recovery scenarios.

## Normal State of Operation

* Network – IP space assigned to virtual machines (VMs) at the Primary Site in Culpeper and replicated to the Disaster Recovery (DR) Site in Miami. The VA NSOC has requested that all programs begin using the native IP space on 10.244.x.x and 10.245.x.x as opposed to the traditional RNAT configuration.
* Storage – Snap mirrors are taken every 15 minutes and replicated between Culpeper and Miami.
* Virtualization – ESX infrastructure is in Miami if program contract includes the VDR product.

## DR States

* Full DR Failover – All programs failover to the DR site in Miami.
* Single Program DR Failover – A single program, or workload, fails over to the DR site in Miami.
* Virtual DR (VDR) Exercise – An exercise to test an application using the Verizon infrastructure at the DR site in Miami.

## Authorization

Failover to the DR site has to be authorized by the VA and sent to Verizon in writing, preferably via e-mail. In an emergency, a request can be made in person or by telephone once the authorizer’s identity has been properly verified.

## Comparison of VDR Exercise and DR Failover

Table 1: VDR and DR Failover Activities

|  |  |
| --- | --- |
| **VDR Exercise** | **DR Failover** |
| * Scheduled event for testing | * Event related to disaster or degraded service |
| * Primary site remains in production | * DR site becomes production |
| * No impact or risk to the production environment | * Production environment downtime |
| * No production data loss | * Loss of production data\* |
| * No changes to networking required | * Networking changes required |
| * No previous exercise required | * Multiple exercises required recommended prior to failover |

\*Note – Replication occurs every 15 minutes via mirror snapshots. If a full mirror snapshot takes longer than 15 minutes, a delta mirror snapshot is taken at the next 15 minute interval. In the event of an emergency, the snapshot mirror process is interrupted. The DR site is crash-consistent with the primary site, although data at the DR site can be older than 15 minutes.

## Diagram of Primary and Secondary Site Configuration

Figure 2: Data Center Layout



## Configuration Overview

1. NSOC – BPE routing configuration:
   1. In the event of a single program DR failover
      1. Verizon network Accredited Configuration Engineer (ACE) will make any necessary changes to the OSPF route metric for the program. Additional changes:
         1. If a program is using the native IP space, the routes will be modified by VA NSOC to transition to the routing to Miami.
         2. If a program is using RNAT then a DNS change will need to be made by the program owner.
      2. Recovery Time Objective (RTO): 15 minutes or shorter per contract.
   2. In the event of a full DR failover
      1. Verizon network ACE will make any necessary change to the OSPF route metric. Additional changes:
         1. If a program is using the native IP space, the routes will be modified by VA NSOC to transition the routing to Miami.
         2. If a program is using RNAT then a DNS change will need to be made by the program owner.
         3. Routes from Culpeper will need to be added to Miami by VA NSOC if not already in place.
      2. Recovery Time Objective (RTO): 15 minutes or shorter per contract.
   3. During a VDR exercise
      1. No changes to routing are made
2. RNAT configuration (for outbound traffic) allows Verizon load balancers and firewalls to have the same rules for routing between Miami and Culpeper.
   1. In the event of a single program DR of a full DR failover
      1. RNAT will not need to be disabled.
      2. For programs using the 10.153.x.x IP space and RNAT, DNS settings will need to be changed by the program owner.
      3. Once the primary site is operational again, RNAT may need to be activated until production returns to the primary site.
   2. During a VDR exercise
      1. Not changes to RNAT are made
3. Replication
   1. In the event of a single program DR failover
      1. Program owner will need to specify how the mirrors are to be managed during the failover.
   2. In the event of a full DR failover
      1. If Culpeper is unavailable, replication will not be necessary.
   3. During a VDR exercise
      1. Verizon storage ACEs will update then break the mirrors between Culpeper and Miami, allowing Culpeper to operate normally as a production environment while the test is conducted in Miami.

## Single Program and Full DR Failover Procedure

1. The Verizon Network ACE synchronizes the load balancer and firewall rules between Culpeper and Miami.
   1. Performed on a regular basis. Frequency and estimated time to be determined.
2. Verizon network ACE will make any necessary changes to the OSPF route metric.
   1. Estimated time: 1-5 minutes through automation and scripting.
3. VA NSOC or the program owner will need to make changes to networking.
   1. For programs using the VA’s native IP space (10.244.x.x and 10.245.x.x, pending confirmation), the VA NSOC changes routing.
   2. For programs using the other IP space (10.153.x.x, pending confirmation), DNS settings are changed by the program owner.
   3. Estimated time dependent on VA NSOC or program owner.
4. Single program DR failover ONLY
   1. Program owner will need to specify how the mirrors are to be managed during the failover.
   2. If requested, Verizon storage ACEs will reverse mirrors between Culpeper and Miami, allowing Culpeper to operate normally as a DR site while Miami becomes writable for production.
5. Verizon storage ACEs register VMs in the DR environment.
   1. Estimated time: 5-10 minutes
6. The Miami environment is now available for the client’s production environment.
7. Client initiates their application.
8. Verizon will assist in any way possible to ensure the operational stability of the production environment.

## Returning to Primary Site from DR Site

Note: Times subject to change.

1. Routing
   1. In the event of a single program DR failover
      1. Verizon network ACE will make any necessary changes to the OSPF route metric for the program. Additional changes:
         1. Estimated time: 1-5 minutes through automation and scripting.
      2. VA NSOC or the program owner will need to make changes to networking.
         1. If a program is using the native IP space, the route metric will be re-modified by the VA NSOC to transition the routing to Miami.
         2. If a program is using RNAT then a DNS change will need to be made by the program owner.
         3. Estimated time dependent on VA NSOC or program owner.
   2. In the event of a full DR failover
      1. Verizon network ACE will make any necessary changes to the OSPF route metric. Additional changes:
         1. If a program is using the native IP space, the route metric will be re-modified by the VA NSOC transition the routing to Miami.
         2. If a program is using RNAT then a DNS change will need to be made by the program owner.
      2. Estimated time: 15 minutes
2. RNAT configuration (for outbound traffic) will not typically need to be altered to return to normal operation.
   1. If Miami is to remain the primary site then additional RNAT will need to be configured by the program owner in Culpeper through Infinicenter. Verizon network ACE can provide assistance and guidance as needed
3. Replication will be re-enabled by re-establishing the mirrors by the Verizon storage ACEs.
   1. Mirrors can be reversed as needed.
      1. Estimated time to be determined.

## VDR Exercise Prerequisites

Prior to initiating a VDR exercise, a program must have:

* A presence in Miami.
* Be contractually subscribed as a VDR exercise enabled program.

After a DR environment is available for the client in Miami, the program owner is responsible for completing the Enterprise Services Change Control Board (ESCCB) process to allow console access across the VA Business Partners Extranet (BPE).

The IP range can typically be found in Infinicenter. Verizon can provide the IPs to the program owner upon request. Ports 902, 903, and 443 (pending confirmation) need to be opened throughout that range for a program to remotely control VMs in Miami during a VDR.

## VDR Exercise Request Process and Procedure

Verizon requires a ticket to be opened by the TFG-027 client. An e-mail can be submitted via e-mail at least two weeks in advance of the VDR exercise. Currently VDR tests can only be scheduled on Tuesdays from 1PM Easter to 4PM Eastern. The VDR exercise consists of the following activities. Please note that timeframes are project-specific and subject to change:

1. Prior to the date of the exercise, the Verizon Network ACE will synchronize the load balancer and firewall rules between Culpeper and Miami. To prevent any performance issues, only the delta of these rules is replicated from the last sync. If resources allow, this will be performed after business hours.
   1. Estimated time to be determined.
2. ACEs will update then break the mirrors between Culpeper and Miami, allowing Culpeper to operate normally as a production environment while Miami becomes writable for the purpose of testing.
   1. Estimated time: 15-30 minutes
3. ACEs will register VMs in the DR environment prior to the VDR exercise.
   1. Estimated time: 5-10 minutes
4. The Miami environment will now be available to the client for the duration of the exercise.
   1. Estimated time: 1-4 hours.
5. Client initiates the test of their application.
6. The program conducting the test stops VMs or other databases in Miami once the exercise is complete.
   1. Estimated time: 15-30 minutes.
7. The program notifies Verizon of the conclusion of the exercise, signaling an all clear, and authorizes Verizon to sanitize the Miami environment.
8. ACEs sanitize the Miami environment.
   1. Estimate time: up to 1 hour
9. Mirrors between Culpeper and Miami are re-established.
   1. Estimated time: 15 minutes