



## Amendment Approval Form

**Contract Between:**

**Northrop Grumman Systems Corporation**

7575 Colshire Drive  
McLean, VA 22102-7508

and

**The Commonwealth of Virginia**

11751 Meadowville Lane  
Chester, VA 23836

<b>Contract Number</b>	<b>VA-051114-NG</b>
<b>Amendment Number</b>	<b>101</b>
<b>Description of Contract Change</b> – Provide a brief description of contract change	Updates Tier 1 Disaster Recovery to add failover by Eligible Customer request.
<b>Section(s) of CIA Referenced</b> – Identify section(s) of CIA modified, including Attachments and Schedules	<ul style="list-style-type: none"><li>• Appendix 1 to Schedule 3.3 (Cross Functional Services)</li><li>• Addendum 1 to Appendix 1 to Schedule 3.3 (Technical Approach)</li><li>• Addendum 2 to Appendix 1 to Schedule 3.3 (Disaster Recovery Services)</li><li>• Schedule 10.1 (Fees)</li></ul>

This is Amendment No. 101 to the Comprehensive Infrastructure Agreement between the Commonwealth and Vendor originally dated as of November 14, 2005 and as subsequently amended (hereinafter, "Amendment No. 101"). The Commonwealth and Vendor have agreed to modify the Comprehensive Infrastructure Agreement as set forth below. Except as expressly modified in Amendment No. 101, the terms and conditions of the Agreement shall remain in full force and effect. Capitalized terms used but not defined in Amendment No. 101 shall have the meanings assigned to them in the Agreement. Amendment No. 101 will be effective 90 days from the date this Amendment is executed by VITA.

1. In Appendix 1 to Schedule 3.3 (Cross Functional Services SOW), the text of Section 3.1.3.4 before the table of responsibilities is deleted in its entirety and replaced with the following.

"IT Service Continuity and Disaster Recovery Services are the activities required to provide prioritized IT Service Continuity, Disaster Recovery, and Emergency Operations Center management support services for VITA's Critical Infrastructure, including applications, and their associated infrastructure (e.g., CPU, servers, network, data and output devices, End-User Devices) and associated voice and data Networks. The IT Service Continuity and Disaster Recovery Services are described in detail in Addendum 2. The following table identifies IT Service Continuity, Disaster Recovery, and EOC roles and responsibilities that Vendor and VITA will perform. Mainframe Disaster Recovery Services are limited to those services that had been provided by SunGard as of the Service Commencement Date."

2. In Appendix 1 to Schedule 3.3 (Cross Functional Services SOW), the following two rows are added to Section 3.1.3.4 at the end of the table of responsibilities labeled as Table 19 [sic].

<b>IT Service Continuity and Disaster Recovery Roles and Responsibilities</b>	<b>Vendor</b>	<b>VITA</b>
29. Provide detailed requirements for Tier 1 Server and Storage Disaster Recovery Services, including Eligible Customer-specific service planning and configuration through the Work Request process.		X
30. Provision and configure Eligible Customer-specific Tier 1 Server and Storage Disaster Recovery Services as requested through the Work Request process.	X	

3. In Addendum 1 to Appendix 1 to Schedule 3.3, the section entitled "IT Service Continuity and Disaster Recovery Services [Appendix 1 to Schedule 3.3 Section 3.1.3.4]" is deleted in its entirety and replaced with the following.

"IT Service Continuity and Disaster Recovery Services are set forth in detail in Addendum 2 to Appendix 1 to Schedule 3.3 (Disaster Recovery Services)."

4. In Addendum 2 to Appendix 1 to Schedule 3.3, the paragraph under the heading "Overview" is deleted in its entirety and replaced with the following.

"The IT Service Continuity and Disaster Recovery Services (the "Disaster Recovery Services" or "DR Services") are a tiered solution that uses a Business Impact Analysis (BIA) ranking. Vendor will use Disaster Recovery Institute International (DRII) standards and methodologies in performing the DR Services. As used in reference to the DR Services, the term "system" refers to the server platform and includes the server hardware, OS, and hosted data."

5. In Addendum 2 to Appendix 1 to Schedule 3.3, the following sentence is added to the paragraph entitled *"Service Boundaries"* under the heading *"Service and Operational Components."*

"The current DR Service tiers described in this SOW require the primary instance of subscribed systems to be hosted at CESC and the failover/secondary instance hosted at SWESC, as further described in the Disaster Recovery Plan. The Tier 1 DR Service is only available for systems where the primary instance is hosted at CESC and the failover/secondary instance is hosted at SWESC. An Eligible Customer may submit a custom solution request for VITA and Vendor's consideration for disaster recovery support from other locations."

6. In Addendum 2 to Appendix 1 to Schedule 3.3 the second sentence under the heading *"Pre-event Readiness and Recovery Services"* is deleted in its entirety and replaced with the following.

"They will work with staff to identify and prioritize the affected systems requiring immediate restoration and implement the Disaster Recovery Plan."

7. In Addendum 2 to Appendix 1 to Schedule 3.3 the second sentence under the heading *"Post-disaster Assessment and Recovery Services"* is deleted in its entirety and replaced with the following.

"Work with staff to identify and prioritize the affected systems requiring immediate restoration and implement the Disaster Recovery Plan."

8. In Addendum 2 to Appendix 1 to Schedule 3.3 under the heading *"Testing Service Level Capabilities and Frequency,"* the two sentences that read *"The annual DR test is comprised of a Hot-site failover from the Production site to the DR site with a fail-back test from the DR site to the Production site. Testing a failover of Production to DR site will include production datacenter plus remote operations that fall under a DR-service option."* are deleted in their entirety.

9. In Addendum 2 to Appendix 1 to Schedule 3.3 the paragraph under the heading *"Network Services"* is deleted in its entirety and replaced with the following.

"All required network components are in place in CESC and SWESC for site failover. This would include all internet-facing connection technology utilizing dedicated virtual private networks as well as SONET, frame relay, or Internet (public) VPNs. Firewalls and virtual local area networks will be defined in the production site as well as in the DR site enabling resource isolation in both environments. Vendor will leverage Vendor's capacity management tools and processes to support the DR Services and the target system's availability."

10. In Addendum 2 to Appendix 1 to Schedule 3.3 the first four sentences under the heading *"Operational Considerations—Scalability, redundancy, reliability, performance, availability, manageability: Dedicated Model"* are deleted in their entirety and replaced with the following.

"SWESC is the DR site and will have storage access over the SAN. Servers will be dedicated and may be in a cluster for high availability for data storage."

11. In Addendum 2 to Appendix 1 to Schedule 3.3, the first two paragraphs under the heading *"Technical Description"* are deleted in their entirety. The sentence that reads *"There are six Tier-Level DR Solutions:"* is deleted in its entirety and replaced with the following.

"An Eligible Customer may select from one of six tier-level DR Services:"

12. In Addendum 2 to Appendix 1 to Schedule 3.3, under the heading *"Technical Solution"* the section entitled *"Tier 1 and 2"* is deleted in its entirety and replaced with the following.

**“Tier 1**

- **Service Boundaries:** An authorized representative of an Eligible Customer subscribed to Tier 1 DR Services may request failover to SWESC of such Eligible Customer’s systems receiving Tier 1 DR Services. Vendor will work with the subscribing Eligible Customer to create and maintain an Eligible Customer-specific Disaster Recovery Plan, including the procedure to submit a request to invoke failover for each system subscribed to Tier 1 DR. For each system subscribed to Tier 1 DR Services, Vendor requires a minimum of four hours from incident reporting in order to attempt resolution prior to initiating failover; however, Vendor will initiate the requested failover with approval from Commonwealth’s CIO or the VITA Director of Service Management and Delivery (or if either is unavailable, approval from two of the CIO’s direct reports) before such minimum of four hours passes. Eligible Customer-requested failover is not to be used as a resolution path or “quick fix” for systemic issues resulting from configuration or capacity management issues associated with Eligible Customer mission-critical environments. Failback from the DR Tier 1 solution will require the Eligible Customer follow the standard non-emergency change request process.
- **Database Recovery Considerations:** Database servers will be recovered to a physical or virtual server at SWESC, servers may be on a high availability cluster configuration if required. Recovery areas may be configured that can be leveraged for flashing/rolling back database transactions in the event of logical errors. Replication technology utilizing snapshot or rollback features may be used to recover from physical corruption. Consistency groups will be used to maintain consistency between the database files (data, journal, and log) and prevent data corruption. The mirrored or replicated files will be in a consistent and start-able state at SWESC.
- **Server Recovery Considerations:** Systems marked for recovery will be maintained in active/passive failover configurations. All systems marked for recovery will have the primary instance of the system hosted at CESC and the failover/secondary instance of the system hosted at SWESC. Failover systems will be configured in a manner to allow implementation of current platform specific tool sets that can be leveraged to minimize the impact of hardware failure or degraded application performance resulting from secondary system outages.
- **Storage Recovery Considerations:** Systems marked for recovery can be configured with non-locally attached storage, such as SAN hosted storage or a similar storage solution. All systems marked for recovery with non-locally attached storage will have the primary instance of the storage hosted at CESC and the failover/secondary instance of the system hosted at SWESC. Failover storage will be configured in a manner to allow implementation of current storage solution toolsets that can be leveraged to minimize the impact of hardware failure or degraded application performance resulting from secondary system outages.
- **Operational Recovery:** Operational recovery for subscribed systems is achieved through the use of high availability infrastructure and associated services such as the use of asynchronous storage replication and clone technologies.
- **Data Protection:** Application data stored on the CESC production SAN will be replicated to the SWESC SAN using asynchronous remote replication capabilities. Production data will

be available on high available/redundant storage at CESC. In some particular situations, there are requirements to have parts of the data recovered through data replication and parts of the data recovered through backup to Virtual Tape Library (VTL) with the backed up files transmitted over the network to SWESC.

- **Server Configuration:** Systems marked for recovery that are configured for either an active/passive or active/active configuration will have dedicated resources reserved at CESC and SWESC as set forth in the Disaster Recovery Plan. Resource types will be detailed in the architectural solution and based on system requirements provided by the designated application owner. All resources will be configured with appropriate redundancy as defined by the current DR Tier1 Service offering.
- **Failover:** Failover will be performed from a virtualized server environment to a virtualized server environment or from a physical server environment to a physical server environment or from a physical server environment to a virtualized server environment. The last option has the potential to increase the application response time once several physical servers will be running simultaneously in the same virtualized server hardware

## Tier 2

- **Database Recovery Considerations:** Database servers will be recovered to physical or virtual server at SWESC; servers may be on a high availability cluster configuration if required. Recovery areas may be configured that can be leveraged for flashing/rolling back database transactions in the event of logical errors. Replication technology utilizing snapshot or rollback features may be used to recover from physical corruption. Consistency groups will be used to maintain consistency between the database files (data, journal, and log) and prevent data corruption. The mirrored or replicated files will be in a consistent and start-able state at the SWESC.
- **Server Recovery Considerations:** The environment is comprised of physical and virtual servers and connected to the SWESC SAN. Servers are racked and ready for booting. Operating system boot images are pre-loaded or readily available. Applications are loaded. If required, physical or virtual servers are configured into clusters with support for active-active or active-passive configurations.  
Three failover configurations exist:
  - 1.) Physical to Physical – the servers are recovered to a dedicated environment.
  - 2.) Physical to Virtual – the servers are recovered to a shared virtual environment.
  - 3.) Virtual to Virtual – the servers are recovered to a shared virtual environment.
- **Storage Recovery Considerations:** The storage array will be replicated to SWESC using an array based asynchronous replication. Replication frequency will be configured to enable lower Recovery Point Objectives (RPO). Cloning technology will be used to increase application availability and reduce downtime to perform parallel processing activities, for example, backups if required. Snap technology may be used to create pointer-based, space-saving snapshot copies. Consistency groups will be used to maintain multiple Logical Unit Number (LUN) replications in a consistent state, enabling fast recovery and avoiding data corruption at SWESC.
- **Operational Recovery:** Operational recovery for subscribed systems is achieved through the use of high availability infrastructure and associated services such as the use of asynchronous replication and clone technologies.

- **Data Protection:** Application data stored on the CESC production SAN will be replicated to the SWESC SAN using asynchronous remote replication capabilities. Production data will be available on high available/redundant storage at CESC. In some particular situations, there are requirements to have parts of the data recovered through data replication and parts of the data recovered through backup to Virtual Tape Library (VTL) with the backed up files transmitted over the network to SWESC.
- **Server configuration:** For a dedicated server option, the servers will already be racked and installed with the respective operating system and application, ready to initialize when the data logical unit is connected. For a repurposed server option, the servers will be made available from a pre-defined pool of servers which will need to be connected and re-built to the application requirements prior to connecting the logical unit with the application data. A bare metal restoration process can be used to accelerate the recovery time.
- **Failover:** Failover will be performed from a virtualized server environment to a virtualized server environment or from a physical server environment to a physical server environment or from a physical server environment to a virtualized server environment. The last option has the potential to increase the application response time once several physical servers will be running simultaneously in the same virtualized server hardware.

The diagrams below describe the solution for both Tier 1 and 2.”

13. In Addendum 2 to Appendix 1 to Schedule 3.3, Figure 1, the “Server Type” for Tier 1 is changed from “Physical” to “Physical/Virtual.”

14. In Addendum 2 to Appendix 1 to Schedule 3.3, under the heading “Architecture” the second sentence that reads “Section 1.2 defines the DR Service Tier-Level criteria for each Tier along with a high-level solution diagram.” is deleted in its entirety.

15. In Addendum 2 to Appendix 1 to Schedule 3.3, the section entitled “Security / Authentication” is deleted in its entirety.

16. In Addendum 2 to Appendix 1 to Schedule 3.3, under the section entitled “Technical Assumptions” the third bullet is deleted in its entirety and replaced with the following.

“All information identified in the Disaster Recovery Plan will be made available at SWESC.”

17. In Addendum 2 to Appendix 1 to Schedule 3.3, under the section entitled “Technical Assumptions” the two sentences that read “The annual DR test is a Hot-site failover test from the Production site to the DR site, with a fail-back test from the DR site to the Production site. Testing a failover of Production to DR site will include production datacenter plus remote operations that fall under a DR-service option.” are deleted in their entirety.

18. In Schedule 10.1, Fees, the following sentence is added to the end of Section 5.3.10(a).

“Beginning on the effective date of Amendment No. 101, the Fixed Rate Volume-Based Fees for all Tier 1 Disaster Recovery Server Resource Units shall be excluded from the above calculations.”

[SIGNATURES APPEAR ON THE NEXT PAGE]

The Parties have executed this Amendment No. 101 on the dates indicated below.

VITA for the Commonwealth of Virginia	Northrop Grumman Systems Corporation
By: 	By: 
Name: Perry Pascual	Name: Roxanne Esch
Contract Manager	Director, Contracts
Date: 5/16/2014	Date: April, 28, 2014