



## Comprehensive Infrastructure Agreement Amendment Approval Form

**Contract Between:**

**Northrop Grumman Information Technology, Inc.**  
7575 Colshire Drive  
McLean, VA 22102-7508

and

**The Commonwealth of Virginia**  
110 South Seventh Street  
Richmond, Virginia, 23219

|  |  |
|--|--|
| <b>Contract Number</b>   | VA-051114-NG   |
| <b>Amendment Number</b>  | Number 51  |
| <b>Section(s) of CIA Referenced – Identify section(s) of CIA modified, including Attachments and Schedules</b> | Addendum 4 to Appendix 3 of Schedule 3.3, Statement of Technical Approach for Security Services:<br><br>Enterprise Security Operations Center<br>Physical Security<br>Centralized Security Incident Response Center<br>Enterprise Identity Management Solution |
| <b>Description of Approved Contract Change – Provide a brief description of contract change</b>                | Paragraph "Enterprise Security Operations Center": Change location of ESOC<br><br>Other paragraphs change the name of CESC from "Richmond Enterprise Solutions Center" to "Commonwealth Enterprise Solutions Center", to align with past amendment.            |



**In accordance with Section 27.5 Amendments, and pursuant to the mutual agreement of the parties, this AGREEMENT is modified as follows:**

**The following four paragraphs of CIA Addendum 4 to Appendix 3 of Schedule 3.3 (Statement of Technical Approach for Security Services), are hereby amended as specified below.**

**All terms, conditions and provisions remain unchanged except as specifically noted herein.**

## **Enterprise Security Operations Center**

Northrop Grumman will collocate the Enterprise Security Operations Center (ESOC) and the Centralized Security Incident Response Center (CSIRC) at the Commonwealth Enterprise Solutions Center (CESC). The backup ESOC and CSIRC will provide redundant capability and are located at the Southwest Enterprise Solutions Center (SWESC). The primary and back-up are separated by a distance of more than 100 miles. Security systems monitor entry into the CSIRC and the ESOC facilities located in both CESC and SWESC; Radio Frequency Identification (RFID) badge reader allows access. The CSIRC and ESOC access are protected additionally by a biometric/card reader combination. This will provide appropriate security staff and leadership has access to the security systems and data within, as well as being protected by the initial defense layer at the building entrance. Further, audit records are available to track who enters and exits.

The ESOC focuses its 24x7 effort on real-time, proactive monitoring, assessing and analyzing the security posture of the VITA Enterprise. Defense of the Commonwealth includes all activities classified as security events, eventually becoming categorized as a threat or non-threat. Upon the determination of active incident status, the ESOC elevates the information to the CSIRC for action and tracking. The two teams of personnel will be cross-trained on ESOC and CSIRC duties. The ESOC staff will monitor, manage, and maintain all security-related technologies including antivirus, firewalls, IDS/IPS, content filtering, network scanning, and identification management capabilities. They will assist VITA in the creation and maintenance of the VITA Security Plan, a detailed account of the IT security efforts within the enterprise with emphasis on the configuration management, change control, risk assessment, and vulnerability assessment plans.

The ESOC shall contribute to VITA IT security awareness by monitoring, assessing, responding, and managing security operations for the VITA Enterprise.

## **Physical Security**

Both VITA data center locations (Commonwealth Enterprise Solutions Center and Southwest Enterprise Solutions Center) will use Northrop Grumman physical security techniques.

The physical security will input data into the ESOC in the form of logs that can be audited, as well as input data into the SITMS, where incidents are tracked and managed by the CSIRC.

## **Centralized Security Incident Response Center**

The CSIRC is located at the Commonwealth Enterprise Solutions Center and is responsible for all security incidents 24x7. The CSIRC will help VITA and executive branch agencies to comply with Code of Virginia § 2.2-603.G. They track, support and maintain user or machine reported incidents by entering the data into the SITMS.

The CSIRC staff is responsible for keeping abreast of all advisories from industry, such as US-CERT, as well as investigating security incidents, focusing on sequence, source and time of events. The CSIRC staff will also maintain industry connections, which enables evaluation of global threat conditions with detailed analyses tailored for VITA needs. In addition to reviewing industry information, they review audit logs and reports and conduct forensic operations when necessary. The outcome of their response generates bulletins to be used by VITA Leadership, system administrators, Information Security System Officers (ISSOs) and network administrators. The bulletins contain status, remediation or recommended actions for the security incident, as well as mitigation plans to prevent future occurrence of events. The bulletins are displayed within the VITA Enterprise Dashboard and provide the ability to perform compliance reporting on bulletin remediation status.

The CSIRC is staffed by dual-trained personnel with capabilities of operating both CSIRC and ESOC systems. Those operations are detailed in standard operating procedures, and the staff is required to attend internal refresher training on both CSIRC and ESOC responsibilities.

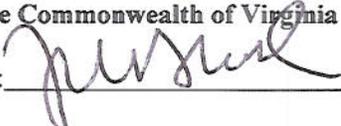
### Enterprise Identity Management Solution

Northrop Grumman will provide an Enterprise Identity Management Solution (EIMS) through a combination of the physical identity credentialing for Commonwealth Enterprise Solutions Center/Southwest Enterprise Solutions Center access and Active Directory.

The parties have executed this Agreement on the dates indicated below.

**Executed by:**

The Commonwealth of Virginia

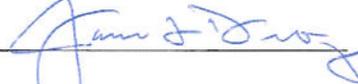
By:  \_\_\_\_\_

Name: Fred Duball

Title: SMO Director

Date: 5-15-08

Northrop Grumman Information Technologies, Inc.

By:  \_\_\_\_\_

Name: James L. Dietz

Title: Senior Contract Manager

Date: 5-13-2008