



## 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>118</b>
<b>Description of Contract Change – Provide a brief description of contract change</b>	Adds Workplace Collaboration Service Multifactor Authentication (WCS MFA)
<b>Section(s) of CIA Referenced – Identify section(s) of CIA modified, including Attachments and Schedules</b>	<ul style="list-style-type: none"><li>• Appendix 13 to Schedule 3.3 (Other Services SOW)</li><li>• Addendum 1 to Appendix 13 to Schedule 3.3 (Other Services Technical Approach)</li><li>• Schedule 10.1 (Fees)</li></ul>

This is Amendment No. 118 to the Comprehensive Infrastructure Agreement between the Commonwealth and Vendor originally dated as of November 14, 2005 and as subsequently amended (hereinafter, "Amendment No. 118"). The Commonwealth and Vendor have agreed to modify the Comprehensive Infrastructure Agreement as set forth below. Except as expressly modified in Amendment No. 118, the terms and conditions of the Agreement shall remain in full force and effect. Capitalized terms used but not defined in Amendment No. 118 shall have the meanings assigned to them in the Agreement.

1. In Appendix 13 to Schedule 3.3 (Other Services Statement of Work), a new section is added as follows.

**"Statement of Work for Workplace Collaboration Service Multifactor Authentication**

Vendor will install, configure, support, and maintain a centralized infrastructure to provide advanced authentication to network accessible Eligible Customer application resources in accordance with the technical approach (hereinafter, "Workplace Collaboration Service Multifactor Authentication" or "WCS MFA"). The Eligible Customer's network accessible applications must be capable of working with WCS MFA. As requested through the Work Request process, Vendor will implement WCS MFA for a subscribed Eligible Customer on a per-network accessible application resource basis. Each network accessible application resource must be associated with an active directory group in the COV domain or the EADS directory identifying users with access to the network accessible application. All End-Users accessing the network accessible application resource, via the intranet or internet, will be required to enter a one-time use password (OTP) in addition to default authentication criteria requirements. Vendor will provide the OTP to End-Users via the Eligible Customer-defined method of Short Message Service (SMS) text to End-User cellular device or via a valid COV email address managed and maintained by Vendor. In order to receive OTP via SMS, End-Users must have a cellular device capable of receiving SMS messages and a valid subscription from a cellular service provider; WCS MFA does not include costs associated with standard messaging rates incurred by the End-User from its cellular service provider. WCS MFA includes enterprise software licensing and software maintenance, but does not include upgrades, except for patches and other updates provided to Vendor at no additional charge. The WCS MFA Fee applies to each unique End-User account associated with each application group.

The table below identifies the roles and responsibilities that Vendor and VITA will perform with respect to WCS MFA.

**WCS MFA Roles and Responsibilities**

<b>WCS MFA Roles and Responsibilities</b>	<b>Vendor</b>	<b>VITA</b>
1. Design and recommend standard provisioning levels and workflow for the enterprise WCS MFA.	X	
2. Review and approve standard provisioning levels and workflow for the enterprise WCS MFA.		X
3. Provide detailed requirements for an individual WCS MFA deployment through the Work Request process.		X
4. Deploy WCS MFA for specified Eligible Customer resource and End-Users as specified in the Work Request.	X	

WCS MFA Roles and Responsibilities	Vendor	VITA
5. Provide detailed requirements for customized WCS MFA workflow deployments through the Work Request process.		X
6. Implement customized WCS MFA workflow for Eligible Customers as specified in the Work Request.	X	

The table below identifies the Service Levels that apply to WCS MFA.

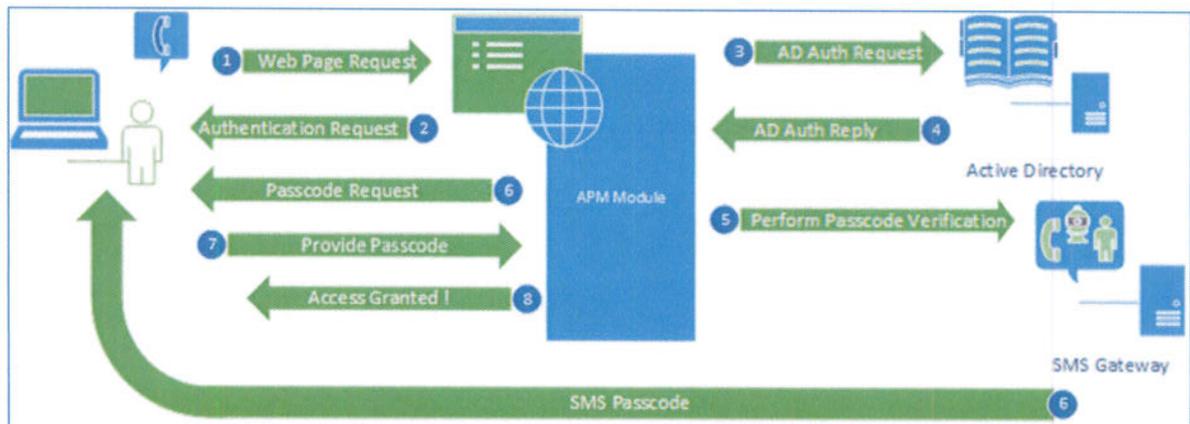
**Service Level for WCS MFA**

Type	Service Level Agreement
Incident Resolution	Priority 2 – Other Locations”

2. In Addendum 1 to Appendix 13 to Schedule 3.3 (Other Services Technical Approach), a new section is added as follows.

**“Technical Approach for Workplace Collaboration Service Multifactor Authentication**

WCS MFA works as illustrated in the diagram below. WCS MFA will prompt the End-User to request a one-time use password (OTP); the OTP will be delivered via email or cellular phone. WCS MFA will access the End-User mobile number stored in the COV Active Directory or EADS directory via a Vendor specified field.



The Eligible Customer is responsible for requesting WCS MFA through the Work Request process. In order to implement WCS MFA, each Eligible Customer is required to identify the following to Vendor in the Work Request:

- Eligible Customers’ network accessible application being subscribed to WCS MFA
- Application group containing End-Users requiring access to the resource
- Requested OTP delivery method (SMS, email, or both)

Vendor will work with the Eligible Customer to test, validate and implement WCS MFA via the Vendor-developed default workflow or a custom workflow based on provided requirements. A WCS MFA workflow must be created for each network accessible application resource using WCS MFA. Any changes or customization to a WCS MFA workflow must be submitted through the Work Request process.

The following limitations apply to WCS MFA:

- The Eligible Customer application must be able to integrate with the WCS MFA.
- The End-User must be a valid COV Active Directory user or subscribed to EADS,
- The COV or EADS End-User is required to have a valid COV or EADS email address or a mobile phone number capable of receiving SMS messages.

3. In Attachment 10.1.3-A to Schedule 10.1 (Definition of Resource Units), the following rows of new text are inserted at the end of the "Other Services" Section (the header row is shown for context only).

Other Services	Unit	Definition
Workplace Collaboration Service Multifactor Authentication (WCS MFA) User	Per WCS MFA User	Monthly recurring Fee for each unique End-User and application group combination authorized to access a WCS MFA resource.
Workplace Collaboration Service Multifactor Authentication (WCS MFA)	Per Project (One-time)	Time and Materials charges for each initiation or change to each WCS MFA workflow.

4. In Attachment 10.1.4-B to Schedule 10.1 (Additional Resource Unit Baselines) the following row of new text is inserted at the end of the "Other Services" Section (the header row is shown for context only). The values for the periods prior to Contract Year 10 shall be "N/A." The values for Contract Years 10 through 13 shall be "0."

Other Services	Unit
Workplace Collaboration Service Multifactor Authentication (WCS MFA) User	Per WCS MFA User

5. In Attachment 10.1.5-A to Schedule 10.1 (Post-Transition Phase Fees - Fixed Recurring Fees and Baseline Resource Unit Rates by Service Tower) the following row of new text is inserted at the end of the "Other Services" Section. The values for the periods prior to Contract Year 10 shall be "N/A." The values for Contract Years 10 through 13 are as shown below (the header row is shown for context only).

Other Services	Unit
Workplace Collaboration Service Multifactor Authentication (WCS MFA) User	Per WCS MFA User

Year 10	Year 11	Year 12	Year 13
\$1.70	\$1.70	\$1.70	\$1.70

6. In Attachment 10.1.7 to Schedule 10.1 (Post-Transition Phase Fees - Additional Resource Charges (ARC) Rates by Service Tower) the following row of new text is inserted at the end of the "Other Services" Section. The values for the periods prior to Contract Year 10 shall be "N/A." The values for Contract Years 10 through 13 are as shown below (the header row is shown for context only).

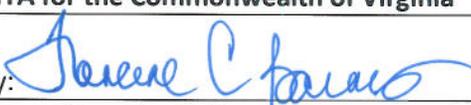
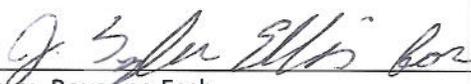
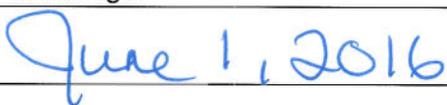
Other Services	Unit
Workplace Collaboration Service Multifactor Authentication (WCS MFA) User	Per WCS MFA User

Year 10	Year 11	Year 12	Year 13
\$1.70	\$1.70	\$1.70	\$1.70

7. In Attachment 10.1.8 to Schedule 10.1 (Post-Transition Phase Fees - Reduced Resource Credits (RRC) Rates by Service Tower), the following row of new text is inserted at the end of the "Other Services" Section (the header row is shown for context only). The values for all periods through Contract Year 13 shall be "N/A."

Other Services	Unit
Workplace Collaboration Service Multifactor Authentication (WCS MFA) User	Per WCS MFA User

The Parties have executed this Amendment No. 118 on the dates indicated below.

VITA for the Commonwealth of Virginia	Northrop Grumman Systems Corporation
By: 	By: 
Name: Francine C. Barnes	Name: Roxanne Esch
Contract Manager	Director, Contracts
Date: 	Date: 05/20/2016