Georgia

Amendment 04

This amendment by and between the Contractor and State Entity defined below shall be effective as of the date this Amendment is fully executed. To the extent the contract requires the State Entity to issue a Notice of Award Amendment for purposes of exercising the renewal option, this written document shall serve as such Notice of Award Amendment.

STATE OF GEORGIA CONTRACT	
State Entity's Name:	Department of Administrative Services ("DOAS" or the "State")
Contractor's Full Legal Name:	Cisco Systems, Inc.
Contract No.:	99999-SPD-T20120501-0006
Solicitation No./Event ID:	99999-SPD0000071
Solicitation Title/Event Name:	Networking Equipment and IT Infrastructure Products
Contract Award Date:	June 21, 2012
Current Contract Term:	July 1, 2014 – June 30, 2015

WHEREAS, the Contract is in effect through the Current Contract Term as defined above; and

NOW THEREFORE, for good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties do hereby agree as follows:

1. **CONTRACT RENEWAL/EXTENSION.** The parties hereby agree that the contract will be renewed/extended for an additional period of time as follows:

NEW CONTRACT TERM	
Beginning Date of New Contract Term:	July 1, 2015
End Date of New Contract Term:	June 30, 2016

The parties agree the contract will expire at midnight on the date defined as the "End Date of the New Contract Term" unless the parties agree to renew/extend the contract for an additional period of time.

2. **CONTRACT SCOPE.** The parties hereby agree that the contract scope will be expanded to include Cisco Cloud Services and Cloud Managed Service Provider (CMSP) Services (collectively "Cloud Services"), pursuant to Section L.5 (Amendments) of the Contract and Attachment C, State of Georgia Performance Expectations, of the RFP incorporated into the Contract, as further described below. As used herein, "Cisco" shall include Cisco and its Affiliates. "Cloud Provider", shall mean Cisco or CMSP Partner (as defined below), as applicable.

   a. **CISCO CLOUD SERVICES.** Cisco currently offers several cloud-enabled Products and Services on the Contract and currently on Cisco's Global Price List, to include appliances, such as Meraki and Ironport, certain "X as a Service" ("XaaS") offerings, such as Software as a Service and Infrastructure as a Service ("IaaS") as well as other cloud-related offerings such as Cisco Openstack Private Cloud and the Cisco Intercloud Platform. In addition, the parties agree that other XaaS offerings and cloud-related Products and Services may be added to the Contract by mutually agreed upon, written amendment to the Contract. Although certain of these Products and Services are already within contract scope, the parties agree to the following supplemental terms and conditions, which shall be applicable to XaaS offerings and other similar cloud-based services.

      i. **Order Process.**

         1. Subscription-based Cisco Cloud Services may be ordered from Cisco's Global Price List through the User Agency's chosen reseller through the existing order process (i.e., Reseller will provide quotes, process purchase orders, invoice and collect payment) as set forth in Section L.10 (Use of Third Parties) of the Contract.

         2. Statement of Work ("SOW") based Cisco Cloud Services may be ordered from Cisco's Global Price List by entering into a Statement of Work with the User Agency's chosen Reseller for the applicable Cisco Cloud Services. Cisco reserves the right to review and approve the scope of SOW-based Cisco Cloud Services. A sample SOW for Cloud Services is included as Attachment 4A.

         3. Resellers must meet all required Cisco qualifications and certifications and enroll in the relevant partner programs to sell the applicable Cisco Cloud Services. Cisco reserves the right to decline any purchase order or SOW for Cisco Cloud Services to the extent such Cisco Cloud Services require Cisco to comply with applicable telecommunications statutes, regulations or rules that would require Cisco to obtain additional regulatory filings or applications, make modifications to its pre-existing internal procedures or incur additional expenses in the performance of Cloud Services under the Contract.

         4. Resellers must meet all required State of Georgia qualifications and certifications and must work with the end User Agency to adhere to

Georgia Technology Authority SA-14-003 Requirements to Use Cloud Services.

ii. **Service Level Availability.** Cisco will maintain 99.5% availability on the Cloud Services set forth in Attachment 4B, excluding connectivity. ("Availability Level"). Any web-based portal as part of the service is not part of the availability SLA. Additional SLA terms may apply based on the end user agency requirements and service offerings. Additional SLA terms will be negotiated with the end User Agency.

iii. **Down Time Credit**. For any cumulative time periods in excess of that contemplated by Availability Level for which the cloud-based Advanced Services are unexpectedly unavailable to the Internet ("Down Time"), as set forth in more detail in an applicable SOW, Cisco will credit the Reseller the Subscription Service Fees or License Fees, as applicable, owed in an amount equal to that portion of the month attributable to the Down Time; provided that (i) use of the Cloud Services is impacted, (ii) the Down Time is reported within forty-eight (48) of each occurrence, and (iii) the User Agency requests credits not more than thirty (30) days after each occurrence. Scheduled maintenance shall not be considered Down Time. The terms and conditions of this section and the Down Time section of the SOW, if any, shall be the User Agency's sole and exclusive remedy and the Contractor's sole obligation for any Down Time. Any Downtime Credit would be itemized and applied against a future order. The Administrative Fee will be calculated based on the net price set forth in the future order, adjusted for the Downtime Credit (i.e., same process as the current trade in credit adjustment).

iv. **Confidentiality**. To the extent permitted by applicable law, all parties agree that the existence and terms of this SLA and the issuance of any credits in accordance with this SLA, are strictly confidential and shall only be disclosed to the customer or reseller, and to employees of the parties on a "need to know" basis for purposes of fulfilling the parties' obligations hereunder. Neither party will disclose to any third party (other than a purchasing customer) the existence, intent, or terms of this SLA without the prior written consent of the other party.

v. **Credit Availability**. If Cloud Services are prepaid, a Credit Memo will be issued. The Credit Memos described above may be applied by the User Agency toward the purchase of Contractor products or services during the 12 months following issuance of such credits. Any credit not used within such 12 month period shall be void and have no value. Credits may not be converted to refunds, used as set off from any amount owing to Contractor, nor transferred or assigned.

vi. **Licensing and Software Transfer.** Contractor's End User License Agreement and Software Transfer and Re-licensing Policy (as incorporated in Section C.2 of the Contract) shall apply to the Cisco Cloud Services.

vii. **Service Descriptions.** Cisco Cloud Services will be governed by Cisco's Service Descriptions, which will be identified and attached to the applicable SOW, or for Cisco Cloud Services that are sold via Purchase Order (and not SOW-based), such Service Description will be attached to the fulfillment partner's quote for Cisco

Cloud Services. Service Descriptions are available for informational purposes online at http://www.cisco.com/go/servicedescriptions/.

b. **CISCO CLOUD MANAGED SERVICE PROVIDER SERVICES.** A Cisco Authorized Reseller may have its own XaaS offerings running on Cisco-powered infrastructure and based on Cisco recommended and validated architectures ("CMSP Services").

i. **CMSP Services.** The following CMSP Services are available under this Contract:

1. Unified Communications as a Service (UCaaS)
2. Contact Center as a Service (CCaaS) (Note: only available to political subdivisions and other non-state agency Authorized Users)
3. Video/Telepresence as a Service (TPaaS)
4. Disaster Recovery as a Service (DRaaS)
5. Infrastructure as a Service (IaaS)
6. As additional XaaS CMSP Service offerings become available, the parties may add such offerings by amending the contract as mutually agreed upon Cisco and DOAS.

ii. **Partner Eligibility.** The CMSP Services are available for purchase from resellers identified as CMSP Partners and approved by the State. Partners must comply with the requirements set forth in Section 3 below, as well as any supplemental terms set forth in an applicable SOW. As of the Effective Date of this Amendment, the partners set forth in Attachment C have been approved by Cisco and the State to sell CMSP Services. Additional Partners meeting the Partner eligibility criteria set forth herein are eligible to be added to this contract with State approval pursuant to Section L.10 of the Contract. All Data and Cloud Data Centers must be located within the Continental United States ("CONUS"). All partner offerings must include certified Cisco technical support (365X24X7) included as part of the reseller offering. Data, for purposes of this CONUS requirement, shall be defined as customer data stored by Cloud Provider in the Cloud Data Center in the course of delivering the Cloud Services. Incidental data collected from customer as part of maintenance and support shall not be considered Data. A Cloud Data Center shall be defined as the data center housing the servers and other equipment necessary to provide the basic functionality of the Cloud Services, as described in the applicable service description. Other data centers used to store records regarding maintenance and support (even where such records contain customer data), shall not be considered Cloud Data Centers.

1. **SOW Model.** User Agencies will be able to procure the CMSP Services by entering into a SOW with the User Agency's selected CMSP partner. The SOW will identify the relevant Cloud-specific payment terms, which for purposes of that particular SOW will supersede any conflicting payment terms in the Contract. The SOW will also set forth relevant business terms and other technical requirements from the User Agency. For purposes of the purchase and delivery of the CMSP Services, the SOW will provide the User Agency a direct contractual relationship with the CMSP Partner. The terms and conditions of the Contract shall govern each SOW and for purposes of delivery of the services set forth in such SOW, the Cloud Provider will be responsible for all legal obligations of the Contract as if

such Cloud Provider were the prime contractor (i.e., limitation of liability, indemnification, dispute resolution, etc.). The State agrees that Cisco will not be liable for any CMSP Partner's failure or delay in delivery or any other claims or damages related to the CMSP Partner's obligations under the CMSP SOW. A sample SOW for Cloud Services is included as Attachment 4A.

iii. **SKUs**. CMSP Services are sold under the applicable Partner's SKU(s). Applicable CMSP Partner SKUs will be provided in a separate tab on the monthly price list update from Cisco for convenience purposes only. Partner SKU(s) will include "CBC" in the pricing column, indicating that pricing will be determined in a SOW on a case by case basis. Cisco disclaims all liability for inaccurate SKUs received from Partners and any other information from Partners (i.e., CMSP Partner Service Descriptions) related to the CMSP Services subsequently posted on the Cisco pricing website. Customers should verify pricing included in Partner quotes and incorporated in the relevant SOW and should not rely on the CMSP Partner information included on the Cisco contract website.

iv. SLAs. CMSP Partners will maintain 99.5% availability on the CMSP Services set forth in Attachment A excluding connectivity ("Availability Level"). Any web-based portal as part of the service is not part of the availability SLA. Additional SLA terms may apply based on the User Agency requirements and service offerings. Additional SLA terms will be negotiated with the User Agency. CMSP Partners may offer better service levels in their discretion. Any claims for refunds or other remedies under the applicable SLAs will be solely between the CMSP Partner and the User Agency. Cisco disclaims all liability for the requirements of the SLAs related to a CMSP Services SOW.

v. Down Time Credit. For any cumulative time periods in excess of that contemplated by Availability Level for which the cloud-based Advanced Services are unexpectedly unavailable to the Internet ("Down Time"), as set forth in more detail in an applicable SOW, CMSP Partner will credit the User Agency the Subscription Service Fees or License Fees, as applicable, owed in an amount equal to that portion of the month attributable to the Down Time; provided that (i) use of the CMSP Services is impacted, (ii) the Down Time is reported within forty-eight (48) hours of each occurrence, and (iii) the Purchaser requests credits not more than thirty (30) days after each occurrence. Scheduled maintenance shall not be considered Down Time. The terms and conditions of this section and the Down Time section of the SOW, if any, shall be the User Agency's sole and exclusive remedy and the CMSP Partner's sole obligation for any Down Time. Any Downtime Credit would be itemized and applied against a future order. The Administrative Fee will be calculated based on the net price set forth in the future order, adjusted for the Downtime Credit (i.e., same process as the current trade in credit adjustment).

vi. Confidentiality. To the extent permitted by applicable law, all parties agree that the existence and terms of this SLA and the issuance of any credits in accordance with this SLA, are strictly confidential and shall only be disclosed to the customer or reseller, and to employees of the parties on a "need to know" basis for purposes of fulfilling the parties' obligations hereunder. Neither party will disclose to any third party (other than a purchasing customer) the existence, intent, or terms of this SLA without the prior written consent of the other party.

vii. **Credit Availability**. If CMSP Services are prepaid, a Credit Memo will be issued by the CMSP Partner. The Credit Memos described above may be applied by the User Agency toward the purchase of Contractor products or services during the 12 months following issuance of such credits. Any credit not used within such 12 month period shall be void and have no value. Credits may not be converted to refunds, used as set off from any amount owing to Contractor, nor transferred or assigned.

viii. **Service Descriptions.** Each CMSP Partner will have its own service descriptions or program terms (collectively "Service Description") for the approved applicable CMSP Service, which will be incorporated into the SOW. To the extent there is a conflict between the Contract and the CMSP Partner Service Description, the Contract will take precedence. Relevant partner service descriptions will be attached to the applicable quote for CMSP Services. Applicable Service Descriptions will be uploaded on Cisco's contract webpage, which will be updated as additional CMSP offerings become available or additional CMSP Partners are approved to sell under this Contract. For avoidance of doubt, in the event of a conflict with the version posted on Cisco's website, the Service Description attached to a CMSP Services quote will take precedence over the version posted on Cisco's website. Cisco disclaims all liability for any failure to timely update the CMSP Service Descriptions posted on the Cisco contract website.

c. **Reporting.** Contractor will be required to submit reports for sales of Cisco Cloud Services and CMSP Services (collectively "Cloud Services") as set forth in Section A.4 of the Contract. Cisco Cloud Services and CMSP Services will each have a separate tab in the reporting template. The reporting template will indicate the payment terms (i.e., whether the transaction was an annual subscription service paid in advance, and if applicable, how many years of pre-payment Contractor received). To the extent a transaction involves an amendment to an SOW (i.e., increased capacity, renewals, or changed scope of Cloud Services), Contractor will report the amount set forth in the Change Request executed under the SOW or a new Purchase Order accepted by the Partner for the renewal or additional Cloud Services, during the quarter when the Change Request is executed or new Purchase Order is received.

d. **Administrative Fee.** For Cloud Services, Contractor will pay the administrative fee during the quarter the Purchase Order (or Change Request) was accepted by the Reseller or in accordance with the agreed upon delivery schedule in a SOW or subscription pricing arrangement. For example, for a three year Cloud Services subscription paid one year in advance, the administrative fee for the portion allocated to the first year of the subscription will be due in the quarter the initial sale is reported, while the administrative fee allocated to the second and third year will be due in the quarters that the subsequent transactions are reported, respectively.

3. **Partner Eligibility.** Partners selling Cisco Cloud Services shall maintain all required certifications applicable to that particular offering. Partners selling CMSP Services shall have

an active "CMSP – Service Provider" certification at all times during the contract term. An Authorized User may terminate a CMSP SOW for breach for a Partner's failure to maintain the required certification(s). To the extent such SOW is terminated for breach under this Section 3, Cisco will use commercially reasonable efforts to assist the Authorized User in finding another approved CMSP Partner to complete the Term of the CMSP Services. The following cloud services require the Cisco Authorized Reseller to meet the following requirements:

a. Infrastructure as a Service (IaaS)
    i. CMSP Service Provider Certification
b. Unified Communications as a Service (UCaaS)
    i. CMSP Service Provider Certification - HCS
    ii. Advanced Collaboration Architecture Specialization
c. Contact Center as a Service (CCaaS) (Note: only available to political subdivisions and other non-state agency Authorized Users)
    i. CMSP Service Provider Certification - HCS
    ii. Advanced Collaboration Architecture Specialization
    iii. Contact Center Enterprise Advanced Technology Provider certification
d. Video/Telepresence as a Service
    i. CMSP Service Provider Certification – HCS
    ii. Advanced Collaboration Architecture Specialization
    iii. Telepresence Video Advanced Technology Provider certification
e. Disaster Recovery as a Service (DRaaS)
    i. CMSP Service Provider Certification
    ii. Cloud Builder Specialization

As additional XaaS CMSP Service offerings become available, the parties may add such offerings and required certification levels by amending the contract as mutually agreed upon by Cisco and DOAS.

4. SUPPLEMENTAL TERMS AND CONDITIONS APPLICABLE TO CLOUD SERVICES.

a. Term and Termination of Cloud Services
    i. The Term of a Cloud Service offering will be set forth in the purchase order or applicable SOW unless terminated sooner pursuant to this Section 4.

    ii. Termination of a SOW for Cloud Services by User Agency
        1. User Agency may terminate Cloud Services for cause if Cloud Provider has materially breached the terms of this Amendment in Cloud Provider's performance of Cloud Services ordered hereunder and has failed to cure such breach within 30 days of receipt of the applicable Termination Notice; provided that the notice requirement will not apply if the breach is not capable of being cured, or Cloud Provider has refused in writing to cure it; or
        2. User Agency may terminate Cloud Services at any time for convenience, upon delivery of 180 days' prior written Termination Notice and payment of Termination Charges, if any, identified in the applicable SOW.
        3. User Agency may terminate Cloud Services at any time for non-appropriation, upon delivery of 60 days' prior written Termination Notice. In the event on non-appropriation, Termination Charges will not apply.

4. If any Force Majeure Event prevents Cloud Provider from providing Cloud Services for more than 30 consecutive days, User Agency may terminate the applicable Cloud Services, by written notice to Cloud Provider as set forth in this Section 4(b).

iii. Termination of Cloud Services by Cloud Provider

1. If User Agency (i) is in delay with the payment of any undisputed charges, and (ii) fails to make the outstanding payment within a cure period of 30 days of delivery by Cloud Provider of written notice that clearly states Cloud Provider's intention to terminate Cloud Services due to User Agency's failure to pay; or
2. If User Agency has materially breached the Contract of applicable SOW as it applies to such Cloud Services and has failed to cure such breach within 30 days of receipt of the Termination Notice, provided that the notice requirement will not apply if the breach is not capable of being cured or User Agency has refused in writing to cure it.

iv. Termination Notice. A Termination Notice must specify the effective Termination Date and will comply with any notice periods set forth in the Contract.

v. Scope and Impact of Termination. Termination of a particular Cloud Service will not impact any other Cloud Service or the Contract, which will remain in full force and effect. Following the effective date of termination of the Cloud Service, Cloud Provider will not be obligated to continue performing any such Terminated Cloud Services. Upon termination of the Cloud Services, User Agency shall pay all applicable fees and/or Termination Charges (if applicable) owed under the affected purchase order or SOW.

vi. Exit Assistance. Upon termination of a Cloud Service and upon written request by User Agency, Cloud Provider will provide Exit Assistance in accordance with Attachment D (Exit Assistance). If User Agency has requested Exit Assistance, the terms and conditions of the Contract, including User Agency's obligation to pay for such Cloud Services (except no Exit Assistance fees will be owed if User Agency terminates the Cloud Services for breach) will continue to apply to the provision of Cloud Services during the period of Exit Assistance.

b. Ownership and Licenses.

i. All Intellectual Property Rights, Software, Equipment, Confidential Information and Materials belonging to a Party (for purposes of this Section 4(b), Party shall include Reseller) or its subcontractors or Affiliates (i) prior to the Effective Date, (ii) during the Term, which are developed independently of the Contract, and (iii) any improvements, derivatives, or enhancements to (i) and (ii), ((i)-(iii) shall collectively be referred to herein as "Background IP") will remain vested in that Party, and the other Party shall have no rights other than as expressly granted by this Contract. In addition, each Party assigns its rights in the other Party's Background IP to the extent that ownership is not automatically granted consistent with this Section. Other than the above, nothing in the Contract will be deemed to assign or transfer any Intellectual Property Rights between the Parties.

ii. Except as expressly described herein, nothing in the Contract or any Cloud Services SOW shall alter or affect the Intellectual Property Rights and/or licenses provided with any Cisco Products. The terms and conditions provided with the Licensed Materials (if applicable) or the EULA, are incorporated into Section C.2 of the Contract.

iii. If User Agency is required to use any Third Party Software in the course of receiving the Cloud Services, then User Agency bears the sole obligation to comply with the terms of any such Third Party Software license terms.

iv. User Agency hereby grants Cloud Provider a limited, non-transferable, royalty free, worldwide license to use, copy, process and distribute the Content as reasonably required to provide the Cloud Services.

v. The Cloud Services will not include or contemplate any joint development of any Intellectual Property Rights. To the extent either Party identifies a reason to engage in any joint development activity, the Parties will execute a separate written agreement governing such joint development.

vi. All rights not expressly granted in the Contract are reserved.

c. Confidential Information. In addition to Section F (Confidentiality) of the Contract, the following additional terms shall apply to Cloud Services:

i. User Agency acknowledges that User Agency Confidential Information may not be logically isolated from data of Cloud Provider's other customers or suppliers. Cloud Provider agrees that (i) prior to any disclosure of or access being granted to any co-mingled third party data, including, unless required by law pursuant to any legal obligations to disclose third party data, the User Agency Confidential Information will be severed from and not disclosed in connection with the third party data; and (ii) Cloud Provider is capable of readily locating and/or destroying User Agency's Confidential Information in accordance with this Section 4.

ii. Residual Knowledge. Nothing in this Amendment will prevent either Party from using for itself or others (including providing, without limitation, the same or similar services, products or technology to any others) any general concepts, ideas, know-how, methodologies, processes, techniques or algorithms that were used, developed, or disclosed pursuant to this Amendment and retained in the unaided memories of persons of either Party, provided that in doing so such Party does not: (1) breach its obligations of confidentiality pursuant to this Section 4(c); or (2) infringe the Intellectual Property Rights of the other Party or its Affiliates, including, without limitation, as set forth in Section C.2 (Software Licenses).

iii. Data Usage and Protection. The Data protection obligations and processes are set forth in Attachment E (Security and Data Protection).

iv. Acceptable Use of Cloud Services. User Agency will not use the Cloud Services to:

1. transmit, receive, store or process infringing, obscene, threatening, libelous, defamatory, hateful, false, misleading, fraudulent, unlawful, illegal, or tortious materials, or that violates another party's rights;

2. promote or distribute any viruses, Trojans, worms, root kits, spyware, adware, or any other harmful Software, programs, routines, applications or technologies;
3. perform any actions that it knows or believes may disrupt the Cloud Services; or
4. attempt to gain unauthorized access to the Cloud Services, Cisco's networks or Reseller's networks.

d. Cooperation. Each Party will, to the extent reasonably requested by the other Party and permitted by Applicable Laws, provide reasonable assistance and support to, and communicate and cooperate with, any other supplier that provides services to the other Party in connection with the provision of Cloud Services. Such cooperation includes, but is not limited to following generally accepted industry practices to cooperate with one another when working with the other Party's suppliers in a multi-vendor environment. If there is a material cost for such cooperation, User Agency will pay the costs for such cooperation at rates to be mutually agreed in the Change Request Procedure.

e. Usage of User Agency's Sites; Access to Non-Public Systems/Sites

To the extent that any Cloud Equipment will be located on User Agency Sites, additional terms regarding Cloud Provider's access to such Cloud Equipment, risk of loss related to such Cloud Equipment, and the business continuity plan applicable to such Cloud Equipment will be set forth in an SOW.

f. Access to Non-Public Systems or Sites

i. If, while performing Cloud Services (i) Cloud Provider or any of its agents or subcontractors gains any direct or remote logical access or direct physical access to any User Agency computer system (including Equipment and Software) or any physical access to a non-public part of a User Agency Site or (ii) User Agency or any of its agents or subcontractors gains any direct or remote logical access or direct physical access to any Cisco computer system (including Equipment and Software) or any physical access to a non-public part of a Cisco Site, then:

1. all such access will be strictly limited to that part of the system, Cloud Provider Site or User Agency Site (as applicable), and will only be carried out in such a manner, as is required for proper performance of the Cloud Services;
2. each Party will comply with all confidentiality requirements set forth in Section F of the Contract, and security procedures and requirements of Cloud Provider or User Agency pursuant to the Security Appendix to the applicable SOW; and
3. each Party shall advise the other Party promptly, but in any event at least within ten (10) business days after confirmation that a Security Breach impacted the Cloud Services. Security Breach shall mean unauthorized destruction, loss or alteration of or unauthorized access to customer data maintained, accessed or stored by Cloud Provider.
4. each Party take commercially reasonable measures to address the Security Breach in a timely manner.

g. Procedure. The Parties agree that Changes to Cloud Services will be dealt with through the Change Request Procedure. A sample Change Request for subscription-based Cloud Services is included as Attachment 4F. The Change Request process for SOW-based Cloud Services is set forth in Appendix 4B of the sample SOW in Attachment 4A hereto.

h. Business Continuity Plan. Cloud Provider has and will continue to implement business continuity and disaster recovery procedures designed to allow Cloud Provider to resume delivery of the Cloud Services following a force majeure event, or as specified in the applicable SOW.

i. Security Requirements; Investigations

  i. Cloud Provider will comply, and will provide that each of Cloud Provider Personnel will comply, with:
    1. Cloud Provider's internal security standards and Information Security Policies documented in an applicable SOW;
    2. all applicable site-specific security requirements relating to the User Agency Sites, as are specified in an applicable SOW; and
    3. User Agency's internal security standards to the extent that they are applicable to the provision of the Cloud Services and as specified in an applicable SOW.

  ii. In the event the User Agency's site-specific security policies and/or internal security standards change after the Effective Date an applicable SOW or User Agency requests Cloud Provider's compliance with any additional applicable policies provided to Cloud Provider in writing after the Effective Date, the Parties will agree such compliance pursuant to the Change Request Procedure and to the extent that Cloud Provider can accommodate such request but will incur additional costs associated with its compliance with such changes or new policies, the pricing for Cloud Services set forth in the applicable Hosted Service SOW will be adjusted to account for such additional costs, pursuant to the Change Request Procedure. To the extent that such policies conflict with or amend the terms of this Amendment 4 or materially change the Parties' respective risks and liabilities, such policies (or portions of policies) will be followed to the extent they do not conflict with this Section 4.

  iii. The SOW will set forth the order of precedence in the event that any of the terms of the above policies conflict with one another, with regard to the provision of the Cloud Services.

  iv. Security Investigations, Systems, and Audit
    1. The Parties will follow the Security Investigation and Audit obligations and processes set forth in an applicable SOW.
    2. Cloud Provider will provide User Agency with access to Cloud Provider Sites or Cloud Equipment (physical, network, or logical, as specified) only if expressly provided in a SOW. No implied right to access such Cloud Equipment is granted. Any access granted will be subject to Section 7.4 and Cisco's Information Security Policies.
    3. User Agency agrees not to perform or allow to be performed any penetration testing, Service performance benchmarking (e.g. application

response times, etc.), load testing or similar tests on the Cloud Services unless agreed in writing by Cloud Provider. The Parties agree that the results of any such tests will be Confidential Information and may not be disclosed to Third Parties without advance written permission from Cloud Provider.

4. If required in a SOW, and no more than once per calendar year, Cloud Provider will perform an independent audit of its Cloud Data Centers at its expense, and provide a redacted version of the audit report upon request. Cloud Provider may remove its proprietary information from the redacted version. A Service Organization Control (SOC) 2 audit report or approved equivalent sets the minimum level of a third-party audit.

j. Excused Performance. If a force majeure event as described in Section L.37 of the Contract impedes Cloud Provider from providing Cloud Services, Cloud Provider will be entitled to (a) continue to invoice for the Cloud Services not affected, and (b) receive an equitable adjustment in the performance schedule that may be mutually agreed to by the Parties. Accordingly, Cloud Provider's delayed or defective performance or non-performance due to force majeure will not constitute a Cloud Services failure and would not be subject to any right that may be available to User Agency for an unexcused Service failure.

k. Compliance with Law. Each party will comply with applicable law. Any User Agency requested changes to the Cloud Services that would result in Cloud Provider being required to secure specific additional licensing from a governmental authority that Cloud Provider does not hold as of the Effective Date of this Amendment 4 will be addressed via the Change Request Procedure. Nothing in this Amendment 4 or the Cloud Services will require either party to breach any Applicable Laws, including, without limitation, data protection or privacy laws, or require Cisco to provide Cloud Services that would result in Cisco being deemed a common carrier, legal advisor, accountant, or telecommunications provider.

l. Change in Applicable Law. If a change of Applicable Laws after the Effective Date requires a change in the scope of Cloud Services, at Customer's option, Cloud Provider will be entitled to either terminate the Cloud Services or recover any reasonable additional costs it may incur by virtue of the need to change the Cloud Services to comply with any changes to such laws, and in such case the Change Request Procedure will apply. Notwithstanding the foregoing, if the change of the Applicable Law is a Cisco Applicable Law, the cost of the modifications required as a result of such change shall be borne by Cisco. After the Effective Date and during the Term, if there are any changes to any Applicable Laws (including any decisions or interpretations by a relevant court or governmental authority relating thereto) that would restrict Cloud Provider from performing the Cloud Services ("Restrictions"), the Parties will meet to discuss and agree, in good faith, how to address the Restrictions. This may include revision of the scope of Cloud Services to implement a mutually agreeable workaround or the elimination of affected Cloud Services from the scope to address the Restrictions.

m. Definitions: Capitalized terms not defined herein shall have the definitions set forth in the Contract.

i. "Cisco Personnel" means any Personnel employed or engaged by Cisco or Cisco Subcontractors;

ii. "Cloud Provider Sites"means premises that are owned, controlled, or occupied by Cloud Provider and used by Cloud Provider for provision of the Cloud Services;

iii. "Cloud Equipment" means the collective Cisco components owned by Cloud Provider and used by Cloud Provider to provide the Cloud Services to User Agency and any other monitoring tools, testing tools, and administration and management tools used for delivery of the Cloud Services.

iv. "Content" means the data, applications, files and other content that User Agency, stores, processes, uploads, downloads or transmits using the Cloud Services.

v. "User Agency Site" means premises that are owned, controlled, or occupied by User Agency that are made available for use by Cloud Provider or its subcontractors for provision of the Cloud Services (or any of them) on the terms set out in this Amendment 4;

n. In the event of a conflict between the terms, the following order of precedence will apply:

i. The Supplemental Terms in Section 4 of this Amendment 4;

ii. The Attachments of Amendment 4, if applicable;

iii. The Contract;

iv. The SOW; and

v. Any supplemental end user license agreement, as applicable.

o. Except where the Contract, as amended, expressly sets forth a different order of precedence for a particular Section, notwithstanding anything in a SOW, Service Description or supplemental end user license agreement to the contrary, the order of precedence shall be i) the Contract, as amended, ii) the SOW, if any, iii) any supplemental license agreement and then iv) the Service Description(s).

5. **SUCCESSORS AND ASSIGNS.** This Amendment shall be binding upon and inure to the benefit of the successors and permitted assigns of the parties hereto.

6. **ENTIRE AGREEMENT.** Except as expressly modified by this Amendment, the contract shall be and remain in full force and effect in accordance with its terms and shall constitute the legal, valid, binding and enforceable obligations to the parties. This Amendment and the contract (including any written amendments thereto), collectively, are the complete agreement of the parties and supersede any prior agreements or representations, whether oral or written, with respect thereto.

[SIGNATURE PAGE FOLLOWS]

IN WITNESS WHEREOF, the parties have caused this Amendment to be duly executed by their authorized representatives.

CONTRACTOR

Contractor's Full Legal Name: **(PLEASE TYPE OR PRINT)**	Cisco Systems, Inc.
Authorized Signature:	
Printed Name and Tile of Person Signing:	Phil Lozano Director, Finance
Date:	June 29, 2015
Company Address:	170 West Tasman Drive San Jose, CA 95134

APPROVED BY LEGAL

STATE ENTITY

Authorized Signature:	Leslie Lowe
Printed Name and Tile of Person Signing:	Leslie Lowe, Assistant Commissioner
Date:	06/30/2015
Address:	200 Piedmont Avenue Suite 1308, West Tower Atlanta, GA 30334

SOW Ref:

Project ID:
Deal ID:

ATTACHMENT A

[SAMPLE]

CLOUD SERVICES STATEMENT OF WORK
[PROJECT NAME]

This Statement of Work ("SOW") for Cloud Services is entered into between [Cloud Provider full name], a [state of incorporation] corporation having a principal place of business at [address] (["Reseller"/ "Cloud Provider"]), and [Customer], a [public sector agency/higher educational institution/etc.] having a place of business in Georgia at [customer address] ("Customer"), and is entered into as of the date of signature as last written below ("SOW Effective Date").

For convenience, the parties agree this SOW is governed by the State of Georgia Statewide Contract for Network Equipment and IT Infrastructure between the Georgia Department of Administrative Services ("DOAS"), effective June 21, 2012, as amended, between Cisco and (DOAS") ("Contract") with Cisco Reference 64609, DOAS Reference 99999-SPD-T20120501-0006. [if CMSP Services SOW, add: However, Customer agrees that Cisco is not a party to this SOW and has no liability for the Reseller's compliance with the terms or performance of the Cloud Services under this SOW.] The terms of this SOW are limited to the scope of this SOW, and shall not be applicable to any other Statements of Work executed between the parties. Capitalized terms used in this SOW and not otherwise defined shall have the meanings given them in the Contract. To the extent there is a conflict between the terms of this SOW and the Contract, the terms of the SOW shall control with respect to the subject matter of the SOW, unless explicitly stated otherwise in this SOW.

This SOW consists of this signature page and the following sections:

Exhibit 1: Project Scope, Responsibilities and Pricing

Exhibit 2: SOW Process, and Terms & Conditions

Appendix A: Example Milestone Completion Certificate **[Delete if not applicable]**

Appendix B: Example Change Request for SOW-based Cloud Services

AGREED:

Each party, as evidenced by the signature below or electronic signature, as applicable, of its authorized representative, acknowledges that it has read and agrees to this SOW in its entirety.

[Cloud Provider **Full Legal Name]**

By: ______________________

Name: ______________________

Title: ______________________

Date ______________________

[Customer Full Legal Name]

By: ______________________

Name: ______________________

Title ______________________

Date ______________________

[SAMPLE]

CLOUD SERVICES STATEMENT OF WORK
EXHIBIT 1 – PROJECT SCOPE, RESPONSIBILITIES, AND PRICING

1.0 PROJECT SCOPE

Project Name: [Project Name]

End User

Cloud Provider shall provide the following Cloud Services and Deliverables to [Customer name] ("End User") or ("Customer").

1.1 Services

As more fully described in Section 2.0 – "Responsibilities of the Parties", Cloud Provider shall provide the following Cloud Services to End User, during Standard Business Hours, unless explicitly stated otherwise in this SOW.

- **[SKU Reference and SKU description]**

1.2 Scope of Cloud Services

[Type of Cloud Services]
<<Remove this section if there is no Services Summary to include. Please ensure that if you insert a Services Summary, it should only be a high level and necessary description of the services to be provided. This summary is not intended to replace any other section of the SOW>>

1.3 Document Deliverables

As more fully described in Exhibit 2, Section 3.0, Cloud Provider shall provide for review and approval the following Document Deliverables:

- **[Describe, if any or state "None"]**

1.4 Location of Services

Services shall be performed as a combination of remote from Cloud Provider Site(s) and onsite at the following End User (or Integrator) Site(s):

- [Insert location]

1.5 Product Summary

[The Cloud Services performed in accordance with this SOW apply to the Products listed below **OR** in Appendix C: Bill of Materials (BOM). **OR** This SOW does not apply to the purchase of the Products.]

1.6 Services Schedule

The following is the initial schedule of Services:

Service Name/Project Task	**Targeted Commencement Date (Business Days)**	**Targeted Completion Date in Elapsed Time (Business Days)**
[Name of Services] (Remote and On Site)	T0	T0 + 90 Business Days

Services shall not commence until this SOW has been fully executed, Cloud Provider has accepted a valid Purchase Order, and has scheduled the start of Services ("Start Date") or ("T0").

Cloud Provider has a lead time of [Forty-Five (45)] Business Days to schedule the start of Cloud Services. Cloud Provider will notify Customer in writing of the actual commencement date of Cloud Services.

All changes affecting the baseline schedule are subject to agreement by Customer and Cloud Provider and managed through the Change Management Procedures as specified herein.

The final Cloud Services Schedule shall be mutually determined by Cloud Provider and the Customer, and documented in writing.

1.7 Single Point-of-Contact Information

Customer and Cloud Provider shall designate a single point of contact to whom communications in regards to the Cloud Services may be addressed and who has the authority to act on all aspects of the Cloud Services; shall be available during Standard Business Hours; and shall designate a backup contact for when the primary contact is not available.

Cloud Provider Contact Name:		**Customer Contact Name:**	**{. . .}**
Title:		Title:	{. . .}
Telephone Number:		Telephone Number:	{. . .}
E-mail Address:		E-mail address:	{. . .}

2.0 RESPONSIBILITIES OF THE PARTIES

2.1 [Insert Cloud Provider and Customer Responsibilities based on the type of Cloud Services]

Cloud Provider Responsibilities:

Customer Responsibilities:

- If applicable, User Agency has secured an exemption from Georgia Technology Authority's (GTA) SO-10-003 or according the provisions of GTA SA-14-003.

General Customer Responsibilities: [Revise/Delete as relevant to the Cloud Services]

i. Designate a single point of contact to act as the primary technical interface to the designated Cloud Provider engineer.

ii. Ensure key Customer personnel (such as: architecture design and planning, network engineering, network operations staff) are available to participate during the course of the Service (to provide information and to participate in review sessions).

iii. Provide documented Customer requirements (business and technical) and high-level network architecture design specifications.

iv. Provide documented information on Customer's existing network infrastructure design including such as: features and services, route plans, addressing schema, call/data flow, dial plans, security policies, network management and operational processes.

v. Unless otherwise agreed to by the parties, Customer shall respond within five (5) Business Days of Cloud Provider's request for any other documentation or information needed to provide the Cloud Service.

vi. Customer agrees to utilize Collaboration Tools.

vii. The following is required for Customer's use of Collaboration Tools: a). Customer will provide the names and other pertinent information (such as e-mail account information) of Customer resources who require authorization to access; b). Customer will support the implementation of software required to use the Collaboration Tools in their environment; c). Customer will download Collaboration Tools guest client(s), if applicable, if not already in possession of the applicable license; and d). Customer agrees to immediately return Collaboration Tool(s) to Cloud Provider, as instructed by Cloud Provider, upon the earlier of: (i) completion of Services; or (ii) Cloud Provider's request to Customer that the Collaboration Tool(s) be returned to Cisco.

3.0 ASSUMPTIONS

Services and service pricing are based upon the following assumptions and exclusions ("Assumptions"). Any additional costs identified as a result of deviations from these Assumptions will be managed through the Change Management Procedures specified in this SOW. Customer and Cloud Provider agree that any changes in the Assumptions may result in an adjustment in the pricing stated in this SOW.

a. This SOW should be read in conjunction with the SOW General Assumptions and Exclusions document posted at: www.cisco.com/go/servicedescriptions which is hereby incorporated into this SOW by this reference. To the extent there is a conflict between the terms of this SOW and such document, the terms of this SOW shall control.

b. Customer is responsible for determination of its design requirements and the utilization of any recommendations provided by Cloud Provider. Cloud Provider recommendations are based upon Customer information provided by Customer at the time of the services. Cloud Provider shall not be liable for the accuracy or completeness of the Customer provided information contained in the Cloud Provider recommendations.

c. Each party acknowledges that completion of Services by the Targeted Completion Date is dependent upon the other party (each as appropriate and as further described in Section 2.0 above) meeting its obligations in this SOW.

[insert any additional assumptions that are project specific.]

4.0 PRICING

4.1 Pricing Table

Customer will issue Purchase Orders in accordance with the following Cloud Services Pricing scenario.

Services Part Code	Term (months)	Service Description	Unit Price (USD)	Extended Price (USD)
			$INSERT	$INSERT
			Total Price:	$INSERT

Pricing premised upon Cloud Services provided by non-union labor.

4.2 Travel and Expense

Travel and Expense ("T&E") is/is not included, or itemized in the above pricing. [Pricing is for Remote Services only or End User Site is considered to be local and Travel and Expense (T&E) is not necessary. OR To the extent T&E is included, such expenses will be governed by Georgia's State Accounting Office Travel Policy http://sao.georgia.gov/state-travel-policy .

4.3 [Milestone] Invoice Schedule [if billed on a Milestone Basis]

Cloud Services will be invoiced upon completion of each Milestone as set forth in the following Milestone Invoice Schedule (MIS) and in accordance with Exhibit 2, Section 4 "Completion":

Milestone #	Milestone Description	Invoice Amount (USD)
1.		$INSERT
	Total:	**$INSERT**

This MIS supersedes any Milestones identified in a Purchase Order; provided however, the total invoiced amounts for Milestones will not exceed the total amount of Integrator's Purchase Order unless such amounts are mutually agreed upon pursuant to the Change Management Process under Exhibit 2.

Any changes to the MIS will be managed through the Change Management Procedures specified in Exhibit 2 of this SOW.

SAMPLE

CLOUD SERVICES STATEMENT OF WORK
EXHIBIT 2 – SOW PROCESS AND TERMS AND CONDITIONS

1.0 ORDERING AND COMMENCEMENT

1.1 Prior to Cloud Provider performing the Services, Customer must have:

i. A fully executed SOW, and

ii. Issued a valid Purchase Order to Cloud Provider for the Cloud Services.

1.2 The term of each SOW commences on the SOW Effective Date and shall continue until [last Milestone completion or Termination Date].

1.3 The SOW shall be governed by the terms and conditions of the Networking Equipment and IT Infrastructure Products Contract, as amended, (the "Contract") executed by Cisco Systems, Inc. and the Georgia Department of Administrative Services ("DOAS") and shall be interpreted based on the order of precedence set forth in the Contract, as amended. For purposes of delivery of the services set forth in this SOW, the Cloud Provider will be responsible for all legal obligations of the Contract as if such Cloud Provider were the prime contractor. This SOW shall create a direct contractual relationship between the Cloud Provider and the Customer.

2.0 PURCHASE ORDER

Purchase Orders shall be issued to the Reseller and sent to the following:

Cloud Provider Services Manager:	Services Account Manager	Email Address:	Email address

2.1 Purchase Order Issuance:

2.1.1 Customer shall purchase Cloud Services by issuing a Purchase Order to the Cloud Provider, subject to Cloud Provider's acceptance and Cisco's approval of the scope, for the total price identified herein. Each Purchase Order must be signed, if requested by Cloud Provider, or (in the case of electronic transmission) sent, by an authorized representative and indicate the following information:

a. SOW/Project ID Number;

b. Travel and Expense Part No., Price, (if applicable as a separate line item);

c. Total Purchase Price;

d. Bill-to, and Ship-to (Service-to) addresses;

e. Requested Services Start Date; and

2.1.2 All Purchase Orders issued for the Cloud Services identified in this SOW must reference this SOW as well as the Contract number. The terms and conditions of this SOW prevail regardless of any conflicting terms on the Purchase Order, other correspondence and any and all verbal communications.

2.2 Term. The SOW Term shall be from the date of last signature below ("Effective Date") and shall continue until ____ [SELECT 1, 3 or 5 year term based on offering] unless terminated earlier in accordance with the terms of the Contract or this SOW.

2.3 The terms of this SOW including the pricing set forth herein are valid only for a period of sixty (60) calendar days from date of submittal unless fully executed within such period.

2.4 Date of Submittal: [date]

2.5 [Insert details] Services Part No., Quantity, Price, Billing Model (i.e., flat fee, milestone-based, usage based, overage calculations, if any), Payment Due Date(s).

3.0 DOCUMENT DELIVERABLE REVIEW AND APPROVAL PROCESS [IF APPLICABLE – DELETE IF NO DOCUMENT DELIVERABLES]

For Document Deliverables that are subject to review and approval from Customer, the parties will adhere to the following review and approval process:

3.1 Cloud Provider will present the draft Document Deliverable to Customer when the document is ready for review and approval.

3.2 Customer shall review the draft Document Deliverable with Cloud Provider, providing written comment or approval of the Document Deliverable within five (5) Business Days immediately after completion of such review.

3.3 If no written (including email) comment or approval is received by Cloud Provider within said time period, the Document Deliverable as provided by Cloud Provider is deemed to be accepted by the Customer.

3.4 If Customer provides comments, then Cloud Provider shall address such comments in a timely manner and this process for review and approval will be repeated.

3.5 No further Cloud Services as defined in the SOW will be performed until the Customer's acceptance of Document Deliverables is received by Cloud Provider.

4.0 COMPLETION [ONLY APPLICABLE TO MILESTONE BASED SOWS]

Customer's review and approval of all milestones provided to Customer will adhere to the following process:

4.1 Cloud Provider shall notify Customer of Cloud Provider's completion of a Milestone or Service by submitting to Customer a Milestone Completion Certificate ("MCC") (an example of which is provided as Appendix 4A).

4.2 Customer has ten (10) Business Days from the receipt of the MCC to sign and return the MCC to Cloud Provider.

4.3 Customer's signing of the MCC, or Customer's failure to respond to the MCC within the ten (10) Business Day period, signifies Customer's acceptance that Cloud Provider has performed the Cloud Services listed in the MCC in accordance with the SOW.

4.4 To decline acceptance of the MCC, Customer must provide to Cloud Provider in writing that the MCC has been declined, and detail how the Cloud Services have not been performed by Cisco in accordance this SOW.

4.5 Cloud Provider shall address any such non-conformance in a timely manner. Cloud Provider shall compile an action plan to correct any non-conformance and the process for acceptance detailed herein will be repeated until such time as all non-conformances have been resolved. Acceptance may not be declined due to defects in Services that do not represent a material non-conformance with the requirements of this SOW. Any dispute regarding whether a non-conformance is material will be addressed in accordance with Section L.8 (Dispute Resolution) of the Contract.

4.6 Customer shall not delegate or assign the task of accepting or assessing completion of Milestones.

5.0 CHANGE MANAGEMENT PROCEDURES

5.1 It may become necessary to amend this SOW for reasons including, but not limited to, the following:
5.1.1Changes to the scope of work and/or specifications for the Services,
5.1.2Changes to the Milestone Invoice Schedule (MIS), [if applicable]
5.1.3Changes to the project schedule,
5.1.4Unavailability of resources which are beyond either party's control, and/or,
5.1.5Environmental or architectural conditions not previously identified.

5.2 A request for a change may be initiated by either party in accordance with the procedure outlined below:
5.2.1The party requesting the change will deliver a "Change Request" to the other party (an example of which is provided in Appendix B). The Change Request will describe the nature of the change, the reason for the change and details of the likely impact, if any, on the project's schedule, scope, pricing and payment.
5.2.2The parties will evaluate the Change Request and negotiate in good faith the changes to the Services and additional fees, if any, required to implement the Change Request. If both parties agree to implement the Change Request, both parties will sign the Change Request, indicating the acceptance of the changes by the parties.
5.2.3Upon execution of the Change Request, the Change Request will be considered an amendment of this SOW.
5.2.4Cloud Provider is under no obligation to proceed with the Change Request until both parties agree to and sign the Change Request.

5.3 Whenever there is a conflict between a fully executed Change Request and the original SOW, or a previous fully executed Change Request, the terms and conditions of the most recent fully executed Change Request will prevail.

6.0 **SERVICE DESCRIPTION.** The applicable Service Description for the Cloud Services is attached at Appendix __ hereto.

7.0 **SERVICE LEVEL AGREEMENT.** Cloud Provider will provide a minimum Service Level of 99.5% availability as set forth in Section 2(b) of Amendment 4 of the Contract. [To the extent Cloud Provider offers Service Levels in excess of 99.5% availability, insert additional information here, including calculation of Down Time Credit, if applicable.]

8.0 SUPPLEMENTAL DATA PROTECTION OBLIGATIONS [IF APPLICABLE MAY BE NEGOTIATED WITH CLOUD PROVIDER AND CUSTOMER]

8.1 **[Insert customer specific legal requirements here]**

9.0 SUPPLEMENTAL DATA SECURITY OBLIGATIONS [IF APPLICABLE MAY BE NEGOTIATED WITH CLOUD PROVIDER AND CUSTOMER]

9.1 Order of Precedence. In the event that any of the terms of the security policies conflict with one another, with regard to the provision of the Cloud Services, "Cloud Provider's obligation to comply with the conflicting policies will be based on the following order: (i) first, Cloud Provider's security policies, (ii) second, user agency's internal security standards, and (iii) and third, user agency's site-specific requirements, as applicable. [ORDER MAY BE REVISED BASED ON CUSTOMER'S REQUIREMENTS. ANY CHANGE FROM ORDER OF PRECEDENCE SHALL BE DOCUMENTED IN A MUTUALLY AGREED UPON SOW]

9.2 **[Insert customers specific technical security requirements, certifications or third party audit here]**

9.2.1 All non-public data shall be owned by Customer.

9.2.2 Cloud Provider will not use customer data for any purpose that is not customer-related.

9.2.3 [Identify Customer access and import/export rights for Customer Data.]

9.2.4 Cloud Provider will notify Customer in the event that E-discovery, litigation hold, discovery search, or request for access by law enforcement or courts for the above requests. [specify how notification will take place and processes to follow-up on such requests]

9.2.5 Servicing Open Records [if Cloud Provider will host data that is subject to disclosure under open records];

9.2.6 Records Retention for the statutory period – if applicable (i.e., tax records, tax advise)

9.2.7 Advance notice of major upgrades, system changes and maintenance [include in SOW if not already set forth in a Service Description]

9.2.8 Timing notice regarding scheduled outages and data recovery [include in SOW if not already set forth in a Service Description]

9.2.9 [Background checks – identify requirements]

9.2.10 [etc]

9.3 **Encryption in Transit/Encryption at Rest.** Based upon Federal Information Processing Standards ("FIPS") 199, Customer will determine Data, information system categorization. If categorization level is moderate or higher, Data shall be encrypted in transit and at rest [NOTE: with consent of Customer, encryption at rest requirement may be deleted from this Section based on the required functionality of the service offering] and Cloud Provider and Customer shall use commercially available encryption technologies that conform to applicable laws and regulations. Approved encryption methods are limited to those algorithms that have received substantial public review and have been proven effective.

9.4 **Physical and Environmental Security of Data Center(s).** Based on FIPS 199, Customer will determine data, information, and information system categorization. If categorization level is moderate or higher, any physical data center security requirement in addition to those detailed in Attachment 4E, Section 3.6, Security and Data Protection, shall be mutually agreed upon and documented in the SOW.

9.5 **[audit requirements]**

9.6 **[compliance with PCI DSS, HIPAA, FERPA, etc.]**

9.7 **U.S.-Based Data Centers.** Cloud Provider will only store Data on servers located in U.S.-based Cloud Data Centers.

10.0 ADDITIONAL TERMS AND CONDITIONS

10.1 RESELLER CERTIFICATIONS

10.1.1 Reseller confirms is has the appropriate certifications required to sell the Cloud Services ordered hereunder, including the following:

[insert list of relevant Reseller certifications]

10.1.2 [IF CMSP SERVICES] Reseller confirms it is using the Cisco-powered infrastructure and Cisco-validated solution designs in providing the Cloud Services ordered hereunder.

10.2 Technical Requirements **[IF APPLICABLE MAY BE NEGOTIATED WITH CLOUD PROVIDER AND CUSTOMER]**

10.2.1 [insert here: e.g., web-based, SLA Mgt, rapid provisioning, API restful, monitoring and reporting]

10.2.2 Data Portability [insert if applicable]

10.2.3 Workload Portability [insert if applicable]

10.2.4 Monitoring [insert if applicable]

10.2.5 Security Infrastructure [insert if applicable]

10.2.6 Disaster Recovery/Business continuity [insert if applicable]

10.2.7 Data preservation

10.2.7.1 Cloud Provider agrees to store data past termination for [30/60/90, etc.] days in accordance with the terms set forth in Exhibit 4D, Exit Assistance.

10.2.7.2 [Secure data deletion]

10.3 Support

10.3.1 Reseller will engage Cisco to provide 7x24 technical support services on the back end for the Cloud Services.

10.3.2 Reseller will utilize an online portal for a trouble ticket system to track technical support issues.

10.3.3 Reseller will provide "follow-the-sun" model for maintenance and support unless Customer requests US-only maintenance and support through Cisco's classified Technical Assistance Center offering, which may impact the price of the Cloud Services offered hereunder.

10.3.4 [Scheduled Outage and Maintenance Reporting]

10.4 [additional terms to be negotiated as appropriate for the type of Cloud Services offered]

[ONLY APPLICABLE FOR MILESTONE BASED CLOUD SERVICES DELETE IF SOW IS FOR SUBSCRIPTION BASED CLOUD SERVICES]

Please note that this MCC is provided as an example and should not be filled in until relevant services are complete.

SAMPLE

CLOUD SERVICES STATEMENT OF WORK
APPENDIX A: EXAMPLE MILESTONE COMPLETION CERTIFICATE (MCC)

Pursuant to the Statement of Work ("SOW") referenced as Project ID Number: [project ID] between [Cloud Provider name] ("Cloud Provider") and [Customer Name] ("Customer"), Customer hereby certifies, by the signature below or electronic signature, as applicable, of its authorized representative, that the Service Milestone described below has been completed on the date indicated below and in accordance with the terms of the SOW.

Milestone #	Milestone Description	Milestone Completion Date	Invoice Amount {. . .}
1.	Completion of		
	Total:		$

Customer Purchase Order Number	Cloud Provider Sales Order Number	Cisco Part Number	Invoice Amount {. . .}
<Enter PO# Here>	<Enter SO# Here>	<Enter Product Code>	$
<Enter PO#>	<Enter SO# Here>	Travel and Expense (T&E) BS-TEBILLINGS	$

Total Invoice Amount of Services Completed: $

Is this the last Milestone Completion Certificate? (Yes/No): YES/NO

End User:

Integrator has five (5) Business Days from the receipt of this MCC to sign and return this MCC to Cloud Provider.

Integrator's signing of this MCC, or Integrator's failure to return this MCC within five (5) Business Days, signifies Integrator's acceptance that Services listed above have been performed according to the SOW.

Submitted By:

[Cloud Provider]

MCC Submittal
Date: ____________________

Acknowledged and Agreed:

[Customer Name]

By: ____________________

Name: ____________________

Title: ____________________

Date: ____________________

Please note that this CR is provided as an example and should not be filled in until relevant.

SAMPLE

CLOUD SERVICES STATEMENT OF WORK
APPENDIX B: EXAMPLE CHANGE REQUEST (CR)

Pursuant to the Statement of Work ("SOW") referenced ______ as Project ID Number: [project ID] between [Cloud Provider Name] ("Cloud Provider") and [customer name] ("Customer"), both parties hereby agree that this Change Request will amend the SOW.

1. **Change Request Number: CR <#>**

2. **Summary of Change(s) Requested:**
   This should be a clear summary of why the parties are revising the SOW and what is being changed

3. **Detailed Changes to SOW:**
   Do the requested changes and revised or additional services impact or affect the following SOW sections? Where Y, describe and detail any and all changes to the original SOW arising from the revised services by drafting the way the specific SOW section(s) should now read – remember to consider impact of requested changes to accepted and signed-off document deliverables and completed services and project/invoice milestones

Exhibit 1 Section	Y/N	New SOW Language
1.1 Services		
1.2 Document Deliverables		
1.3 Location		
1.4 Project Schedule		
1.5 Project Representatives		
2.0 Responsibilities		
3.0 Project Assumptions/Exclusions		

4.0 Pricing		

4. Cost Impact:

	SOW/Change Request	Services	T&E	Total
a.	Original Value of SOW	<CUR>0.00	<CUR>0.00	<CUR>0.00
b.	Value of Change Request No. 1	<CUR>0.00	<CUR>0.00	<CUR>0.00
c.	New Value of SOW:	<CUR>0.00	<CUR>0.00	<CUR>0.00

5. **Purchase Order Issuance:**
   If PO issuance is applicable, it should be a clear adjustment (increase or decrease as appropriate) to the original PO value

   Customer shall issue a written Purchase Order to Cloud Provider for this Change Request for the amount of <CUR>0.00, or shall amend the original Purchase Order to show an increase/decrease in price to reflect the new SOW value of <CUR>0.00.

Except as changed herein, all terms and conditions of the SOW remain in full force and effect.

Each party, as evidenced by the signature below or electronic signature, as applicable, by its authorized representative, acknowledges that it has read and agrees to this Change Request in its entirety.

AGREED:

[Cloud Provider Name]

By: ______________________

Name: ______________________

Title: ______________________

Date: ______________________

[Customer name]

By: ______________________

Name: ______________________

Title: ______________________

Date: ______________________

ATTACHMENT 4B
Cloud Services governed by Service Level Agreement

Cisco Cloud Services
[to be inserted]

CMSP Services
[to be inserted]

ATTACHMENT 4C
CMSP Partners Approved to Sell CMSP Services

[TBD]

Sample SOW, Exhibit 4D
Exit Assistance

This Attachment D covers Exit Assistance as it relates to termination or expiration of Cloud Services to the User Agency. Cisco disclaims all liability for Reseller's failure to comply with the obligations set forth in a CMSP Services SOW.

Unless otherwise stated, capitalized terms used in this Attachment D have the meanings set forth in the following decreasing order of precedence: this Attachment D, then the meanings set forth in the SOW(s) (as applicable) and then Section 4(m)(Definitions) of Amendment 4. This order of precedence only refers to the meaning of capitalized terms in this Exhibit D and reflects the meaning that will govern in the event of a conflict in the referenced documents. It has no further impact on the general order of precedence pursuant to the Contract.

1. EXIT ASSISTANCE AND TRANSITION ASSISTANCE

1.1 Exit Assistance Services

Upon expiration or termination of the Contract, except for a termination arising from a failure to pay in accordance with the applicable payment terms, Cloud Provider will provide Cloud Services for a time period to be specified in an SOW ("Exit Assistance"), which shall not exceed nine (9) months beyond the effective date of the original expiration or termination of the Contract (the "Exit Assistance Period"), provided that:

(i) User Agency provides ninety (90) days' prior written notice requesting Exit Assistance; and

(ii) User Agency pays the fees for each month of Exit Assistance provided during the Exit Assistance Period, as set forth in the SOW for the applicable Cloud Services, except User Agency will not be required to pay such fees for Exit Assistance in the event User Agency terminated the applicable SOW for breach due to Reseller's failure to maintain the required certifications.

1.2 Notwithstanding the foregoing, in the event that Cloud Provider terminates a SOW due to User Agency's failure to pay applicable fees, Cloud Provider will not provide Exit Assistance Services unless and until:

(i) User Agency cures such failure by paying all such unpaid and undisputed fees and any associated interest and fees (as applicable); and

(ii) pays all fees related to Exit Assistance in advance of Cloud Provider's obligation to deliver such Cloud Services.

1.3 Transition Assistance Services

The Parties agree that Cloud Provider's obligation to perform the assistance and services described in this Section 1.3, as may be reasonably requested by User Agency to enable the transfer of the Terminated Cloud Services to a successor supplier or to User Agency's in-house operations (the "Transition Assistance Services"), is conditioned on the Parties having agreed the scope and cost of providing the same pursuant to the Change Request Procedure set forth in Attachment F, with both Parties acting reasonably and in good faith. Subject to reaching agreement through the Change Request Procedure set forth in Attachment F, Cloud Provider will provide the following agreed Transition Assistance Services during the Exit Assistance Period:

(a) information specified in Section 3 below;

(b) if the performance of any Transition Assistance Services requires the use of Cloud Provider tools, Cloud Provider shall use such tools in performing the Transition Assistance Services;

(b) assist User Agency and the successor supplier in planning the transfer of the provisioning data;

(c) conduct one or more rehearsal(s) of the transfer of data together with User Agency and the successor supplier as necessary to secure the orderly and complete transfer of all provisioning data;

(d) provide consulting assistance to the successor supplier regarding parallel operations testing, additionally Cloud Provider may agree to assist in the execution of parallel operations testing; and

(e) provide User Agency with such reasonable assistance at User Agency's reasonable request from time to time without undue delay to enable it to draft, maintain and update the exit assistance plan

The performance of the Exit Assistance will not relieve Cloud Provider of the responsibility to perform the Cloud Services (including the Terminated Cloud Services up to the Termination Date), in accordance with the Contract.

2. GENERAL

2.1 Cloud Provider will perform the Exit Assistance and Transition Assistance Services, if applicable, in an efficient and orderly manner, as well as in accordance with any other provisions of the Contract applicable to Cloud Services.

2.2 Cloud Provider will provide User Agency with (or delete) the Materials and Data identified in the Contract in accordance with such clause(s) and in the case of a return, in same format that User Agency delivered the Materials or Data to Cloud Provider.

2.3 As requested by User Agency, and subject to the terms and conditions set forth herein and in the Contract, Cloud Provider will use commercially reasonable efforts to cooperate with the successor supplier during the Exit Assistance Period.

3. EXIT ASSISTANCE AND TRANSITION ASSISTANCE DATA

Subject to the Parties agreeing the scope of such information pursuant to the Change Request Procedure, with both Parties acting reasonably and in good faith, Cloud Provider shall use Commercially Reasonable Efforts to provide the following information during the

Exit Assistance Period:

- Summary data and statistics (e.g. regarding service performance) in relation to Customer Data held by Cloud Provider,

- Up -to-date copies of structured information regarding resolved and unresolved Incidents relating to the Cloud Services (i.e. trouble ticket meta-data).

ATTACHMENT 4E
Security and Data Protection

This Security and Data Protection Attachment ("Security Attachment") sets forth the controls that Cloud Provider will use to maintain the security of User Agency Data ("Customer Data") in connection with Cloud Provider's performance of Cloud Services under the Contract. These security and data protection terms will apply to each applicable SOW for Cloud Services between Cloud Provider and the User Agency. Cisco disclaims all liability for Reseller's failure to comply with the security and data protection obligations set forth in a CMSP Services SOW.

1. <u>Data Protection Executives; Notices</u>. Each SOW for Cloud Services will identify the Cloud Provider and User Agency executives responsible for the obligations set forth on this Security Attachment ("Data Protection Executives").

   Any notices under this Security Attachment or the Contract regarding obligations related to the Customer Data should be communicated as follows:

   a. communications regarding the day-to-day obligations should be communicated in writing via email or other written notice to each of the Data Protection Executives, and

   b. communications regarding any proposed changes to the terms of this Security Attachment or the terms of a Party's Customer Data obligations under the Contract should be directed as required under the notice provisions of the Contract with copies provided to the Data Protection Executives. No such changes will modify this Security Attachment or the Contract unless agreed by the Parties pursuant to the Change Request Procedure.

2. <u>General Security Practices; Data Centers</u>

   Cloud Provider has implemented and shall maintain appropriate technical and organizational measures to protect Customer Data against accidental loss, destruction or alteration, unauthorized disclosure or access, or unlawful destruction, including the policies, and procedures and internal controls set forth in this Security Attachment for its Personnel, equipment, and facilities at the Cloud Provider Service Locations providing the Cloud Services.

3. <u>Technical and Organizational Security Measures</u>

3.1. Organization of Information Security

a. **Security Ownership**. Cloud Provider has appointed one or more security officers responsible for coordinating and monitoring the security rules and procedures.

b. **Security Roles and Responsibilities**. Cloud Provider Personnel with access to Customer Data are subject to confidentiality obligations.

c. **Risk Management**. Cloud Provider performed a risk assessment before processing the Customer Data or offering the Cloud Services.

d. **SOC Report**. If required in a SOW, Cloud Provider shall perform an independent audit of its data centers at least annually at its expense, and provide a redacted version of the audit report upon request. Cloud Provider may remove its proprietary information from the redacted version. A Service Organization Control (SOC) 2 audit report or approved equivalent sets the minimum level of a third-party audit.

3.2. Human Resources Security

a. **General**. Cloud Provider informs Personnel about relevant security procedures and their respective roles. Cloud Provider also informs its Personnel of possible consequences of breaching its security policies and procedures. Employees who violate Cloud Provider security policies may be subject to disciplinary action, up to and including termination of employment. A violation of this policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with Cloud Provider.

b. **Training**. Cloud Provider Personnel with access to Customer Data receive annual security education and training regarding privacy and security procedures for the Cloud Services to aid in the prevention of unauthorized use (or inadvertent disclosure) of Customer Data and training regarding effectively responding to security events.

   i. Training is provided before Cloud Provider Personnel have access to Customer Data or begin providing the Cloud Services

   ii. Training is regularly reinforced through refresher training courses, emails, posters, notice boards and other training materials.

c. **Background Checks**. Cloud Provider Personnel are subject to criminal background checks.

3.3. Asset Management

a. **Asset Inventory**. Access to Customer Data is restricted to Cloud Provider Personnel authorized in writing to have such access.

b. **Information Classification**. Cloud Provider classifies Customer Data to help identify it and to allow for access to it to be appropriately restricted.

c. **Media Handling**

   Cloud Provider Personnel:

   i. Use trusted devices that are configured with security software (and encrypted);

   ii. Follow Cisco's Trusted Device Standard at (http://wwwin.cisco.com/infosec/policies/standards/trusteddevice.shtml) when accessing Customer Data or when having Customer Data in his/her control;

   iii. Avoid accepting or storing Customer Data on a non-Cisco controlled storage device. This includes smartphones, tablets, USB drives and CDs. If Customer

Data must be accepted this way, Personnel are to immediately transfer such data to his/her Cloud Provider laptop and return the device to User Agency; and

iv. Take measures to prevent accidental exposure of customer data, including using privacy filters on laptops when in areas where over-the-shoulder viewing of customer personal data is possible.

3.4. Personnel Access Controls

a. **Access Policy**. Cloud Provider maintains a record of security privileges of Personnel that have access to Customer Data, networks and network services.

b. **Access Authorization.**

i. Cloud Provider has user account creation and deletion procedures, with appropriate approvals, for granting and revoking access to Cloud Provider systems and networks. Cloud Provider uses an enterprise access control system that requires Personnel revalidation by managers at regular intervals based on the principle of "least privilege" and need-to-know criteria based on job role.

ii. Cloud Provider maintains and updates a record of Personnel authorized to access systems that contain Customer Data.

iii. For systems that process Customer Data, Cloud Provider revalidates access of users who change reporting structure and deactivates authentication credentials that have not been used for a period of time not to exceed six months.

iv. Cloud Provider identifies those Personnel who may grant, alter or cancel authorized access to data, systems and networks.

v. Cloud Provider ensures that, each Personnel having access to its systems has a single unique identifier/log-in.

vi. Cloud Provider maintains strict policies against any shared "generic" user identification access.

c. **Network Design**. For systems that process Customer Data, Cloud Provider has controls to avoid Personnel assuming access rights they have not been assigned to gain unauthorized access to Customer Data.

d. **Least Privilege**. Cloud Provider limits access to Customer Data to those Cloud Provider Personnel performing the Cloud Services and, to the extent technical support is needed, its Personnel performing such technical support.

e. **Integrity and Confidentiality**

i. Cloud Provider instructs Personnel to automatically lock screens and/or disable administrative sessions when leaving premises that are controlled by Cloud Provider or when computers are otherwise left unattended.

ii. Cloud Provider computers and trusted devices automatically lock after a short period of inactivity.

iii. Cloud Provider stores passwords in a way that makes them unintelligible while they are in force.

f. **Authentication**

i. Cloud Provider uses industry standard practices to identify and authenticate users who attempt to access information systems. Where authentication mechanisms are based on passwords, Cloud Provider requires that the passwords are renewed regularly, no less often than every 6 months.

ii. Where authentication mechanisms are based on passwords, Cloud Provider requires the password to be at least eight characters long and conform to very strong password control parameters including length, character complexity, and non-repeatability.

iii. Cloud Provider ensures that de-activated or expired identifiers are not granted to other individuals.

iv. Cloud Provider monitors repeated attempts to gain access to the information system using an invalid password.

v. Cloud Provider maintains industry standard procedures to deactivate passwords that have been corrupted or inadvertently disclosed.

vi. Cloud Provider uses industry standard password protection practices, including practices designed to maintain the confidentiality and integrity of passwords when they are assigned and distributed, and during storage.

3.5. Cryptography

a. **Cryptographic controls policy**

Cloud Provider has a policy on the use of cryptographic controls based on assessed risks.

i. Cloud Provider assesses and manages the lifecycle of cryptographic algorithms, hashing algorithms, etc. and deprecates and disallows usage of weak cypher suites, and mathematically insufficient block lengths and bit lengths

ii. Cloud Provider's cryptographic controls/policy addresses appropriate algorithm selections, key management and other core features of cryptographic implementations.

b. **Key management**. Cloud Provider has procedures for distributing, storing, archiving and changing/updating keys; recovering, revoking/destroying and dealing with compromised keys; and logging all transactions associated with keys.

3.6. Physical and Environmental Security

a. **Physical Access to Facilities**

i. Cloud Provider limits access to facilities where systems that process Customer Data are located to authorized individuals.

ii. Access is controlled through key card and/or appropriate sign-in procedures for facilities with systems processing Customer Data. Personnel must be registered and are required to carry appropriate identification badges.

b. **Physical Access to Equipment**. Cloud Provider equipment that is located off premises is protected using industry standard process to limit access to authorized individuals.

c. **Protection from Disruptions**. Cloud Provider uses a variety of industry standard systems to protect against loss of data due to power supply failure or line interference.

d. **Clear Desk**. Cloud Provider has policies requiring a "clean desk/clear screen" at the end of the workday.

3.7. Operations Security

a. **Operational Policy**. Cloud Provider maintains policies describing its security measures and the relevant procedures and responsibilities of its Personnel who have access to Customer Data and to Cisco systems and networks.

b. **Workstations**. Cloud Provider uses the following controls on its workstations that process Customer Data:

i. anti-malware software and firewalls,

ii. password and screensaver controls with automatic lock of workstation upon idleness,

iii. periodic scans for restricted software (e.g., peer-to-peer),

iv. centralized patch management, and

v. hard disk encryption on laptop devices.

c. **Mobile Devices**. Mobile phones and tablets are protected via a mandatory PIN, restrictions on amount of email that can be stored on the device, and a remote wipe capability.

d. **Data Recovery**. Cloud Provider maintains multiple copies of Customer Data from which Customer Data can be recovered. Cloud Provider stores copies of Customer Data and data recovery procedures in a different place from where the primary equipment processing the Customer Data is located. Cloud Provider has specific procedures in place governing access to these copies of Customer Data.

e. **Logging and Monitoring**. Cloud Provider maintains logs of administrator and operator activity and data recovery events.

3.8. Communications Security and Data Transfer

a. **Networks**. Cloud Provider uses the following controls to secure Cloud Provider networks that access User Agency servers which store Customer Data:

   i. Network traffic passes through firewalls, which are monitored. Cloud Provider has implemented intrusion prevention systems that allow traffic flowing through the firewalls and LAN to be logged and protected 24x7.

   ii. Access to network devices for administration requires a minimum of 128 bit, industry standard encryption.

   iii. Anti-spoofing filters are enabled on routers;

   iv. Network, application and server authentication passwords are required to meet minimum complexity guidelines (at least 7 characters with at least 3 of the following four classes: upper case, lower case, numeral, special character) and be changed at least every 180 days.

   v. Initial user passwords are required to be changed during the first logon. Cloud Provider policy prohibits the sharing of user IDs and passwords.

   vi. Firewalls are deployed to protect the perimeter Cloud Provider network.

b. **Virtual Private Networks ("VPN")**. When remote connectivity to the Cloud Provider network is required for processing of Customer Data, Cloud Provider uses VPN servers for the remote access with the following or similar capabilities:

   i. Connections are encrypted using a minimum of 128 bit encryption.

   ii. Connections from User Agencies to Cloud Provider Service Locations are only established using the Cloud Provider VPN servers.

   iii. The use of two-factor authentication is required.

3.9. System Acquisition, Development and Maintenance

a. **Security Requirements**. Cloud Provider has adopted security requirements for the purchase or development of information systems, including for application services delivered through public networks.

b. **Development Requirements**. Cloud Provider has policies for secure development, system engineering and support. Cloud Provider conducts appropriate tests for system security as part of acceptance testing processes.

3.10. Supplier Relationships

a. **Policies**. Cloud Provider has information security policies or procedures for its use of suppliers. Cloud Provider has agreements with suppliers in which they agree to comply with Cisco's security requirements.

b. **Monitoring**. Cloud Provider monitors service delivery by its suppliers and reviews security against the agreements with suppliers. Cloud Provider manages changes in supplier services that may have an impact on security.

3.11. Information Security Incident Management

a. **Response Process**. Cloud Provider maintains a record of information security breaches with a description of the breach, the consequences of the breach, the name of the reporter and to whom the breach was reported, and the procedure for recovering data.

b. **Reporting**. Cloud Provider will report to a User Agency-designated response center any security incident that has resulted, or could be reasonably suspected to have resulted, in a loss, misuse or unauthorized acquisition of any Customer Data that is likely to result in harm to a Data Subject.

3.12. Information Security Aspects of Business Continuity Management

a. **Planning**. Cloud Provider maintains emergency and contingency plans for the facilities in which Cloud Provider information systems that process Customer Data are located.

b. **Data Recovery**. Cloud Provider's redundant storage and its procedures for recovering data are designed to attempt to reconstruct Customer Data in its original state from before the time it was lost or destroyed.

4. The security measures described in this Security Attachment are Cloud Provider's only responsibility with respect to the security of Customer Data. These measures replace any confidentiality obligations contained in the Contract or any other agreement related to the Cloud Services between Cloud Provider and User Agency with respect to Customer Data.

Attachment 4F
Change Management Procedure
and Sample Change Request Template

This Attachment F covers the Change Request Procedure as it relates to Cloud Provider's provision of Cloud Services. For the avoidance of doubt, Change Request within this Attachment does not refer to the operational aspects of hosting the Cloud Services, which are described in the applicable SOW.

Unless otherwise stated, capitalized terms used in this Attachment F have the meanings set forth in the following decreasing order of precedence: this Attachment F, then the meanings set forth in the SOW(s) (as applicable) and then Section 4(n) of Amendment 4 (Definitions). This order of precedence only refers to the meaning of capitalized terms in this Exhibit C and reflects the meaning that will govern in the event of a conflict in the referenced documents. It has no further impact on the general order of precedence pursuant to the Contract.

1. This Change Request Procedure will be initiated upon the issuance by either Party of a request for a change, in the form provided in Attachment F-1 hereto (a "Change Request"). The Party receiving a Change Request will acknowledge receipt of the Change Request within five (5) Business Days of receipt. The Parties will evaluate all Change Requests without undue delay and will track the progress of all active Change Requests. Agreement of a Change Request must be evidenced by execution of the Change Request by both Partner and User Agency.

2. If a requested change would lead to an increase in the monthly charges or a one-time charge, the Parties will agree on the amount of such one-time charge or increased charges in connection with agreeing to the change.

3. Cloud Provider is not under any obligation to perform work relating to a change prior to the execution of an agreed Change Request.

4. Each Party will bear its own costs in relation to the preparation and/or assessment of any proposed changes.

5. Customer may require Cloud Provider to implement an emergency Change relating to the scope of the agreed Cloud Services and may require Cloud Provider to commence work to implement an emergency change immediately. Any such request of an emergency change, if such request will have a material impact on the Cloud Services currently in production, the Parties will discuss and agree to the detail of an appropriate Change Request as soon as reasonably possible, acting in good faith. In the interim, Cloud Provider will be entitled to charge User Agency for the implementation of the requested change at the Cloud Provider's then-current time and materials rates, plus travel and other related expenses, until a Change Request is fully executed.

6. Change Requests to the Cloud Services, if not deemed to be emergency in nature, should be issued no later than (3) three months prior to the targeted implementation date for the changed Cloud Services in order to give the Parties sufficient time to evaluate the request and plan for implementation. This does not guarantee that all Change Requests can be implemented within three months, accordingly, the delivery schedule for the proposed Change will be agreed and documented by the Parties as part of the Change Request Procedure.

Attachment 4F-1
SAMPLE Change Request Form

<Insert PartnerLogo here>	*Change Request – Contract Change to the* Contract Ref: Schedule: Project Id: DSA ID:

CR – Part A: Initiation **CR No**			
Title: Click here to enter CR Title as per CR Idea Log.			
Initiator:		Counterpart:	
Initiation Date:		Required by:	
Identifier:		Priority: H / M / L	
Details of Proposed Contract Change			
Description of current situation: Describe the current situation that requires a Change to be made in the Cloud Services			
Description of new situation and desired Change: Describe the desired Change and resulting situation			
Business / technical reasons for this CR: Please enter a brief justification why the CR is required.			
Risks if not approved / Benefits to the Business: Describe any risks for not approving this CR, or potential benefits			
Authorized / Rejected by Cisco		**Date:**	

Name:	**Signature:**
Authorized / Rejected by	**Date:**
Name:	**Signature:**

CR Part B: Evaluation **CR no**	**Number of approved person days:** **Project / BAU: yes / no**
Analysis of Contract Change: Describe impacts to the Service as a result of this Change Request	
Deliverables: List and describe the deliverables associated with this CR	
Timetable: Describe the Timetable for implementing this CR.	
Financial implications: Describe the financial implications for implementing this CR.	
Other Relevant Information:	
Authority to Proceed	
Authorized / Rejected by: **Signature:** **Name:** **Date:**	**Authorized / Rejected by Cisco:** **Signature:** **Name:** **Date:**
Authorized / Rejected by **Signature:** **Name:** **Date:**	**Authorized / Rejected by Partner:** **Signature:** **Name:** **Date:**