AMENDMENT NO. 1 TO AMAZON ENTERPRISE CUSTOMER AGREEMENT

This Amendment No. 1 (this "**Amendment**") to the AWS Enterprise Customer Agreement by and between Amazon Web Services, Inc. ("**AWS**") and Regents of the University of Michigan ("**Customer**") is effective as of September 13, 2013 (the "**Amendment Effective Date**"). Unless otherwise defined in this Amendment, all capitalized terms used in this Amendment will have the meanings ascribed to them in the Agreement. The parties agree as follows:

1. **AWS Security.** Section 3.1 ("AWS Security") of the Agreement is deleted in its entirety and replaced with the following:

   3.1 AWS Security. Without limiting Section 10.2 or Customer's obligations under Section 4.2, in accordance with the AWS Security Standards AWS will implement reasonable and appropriate measures for the AWS Network designed to: (i) help Customer secure Customer Content against accidental or unlawful loss, access or disclosure; (ii) comply with the Federal Risk and Authorization Program (FedRAMP) Moderate risk impact level requirements for the Regions and Services identified by AWS as FedAMP compliant (currently EC2, S3, EBS and VPC); and (iii) for the AWS GovCloud (US) region, maintain physical and logical access controls to limit access to the AWS Network by AWS personnel, including employees and contractors, to U.S. persons, as defined by 22 CFR part 120.15 ("U.S. Persons") ((i), (ii) and (iii) collectively the "Security Objectives").

2. **U.S. Persons Restricted Access.** The following Sections 3.1.1 and 3.1.2 are added to the Agreement:

   3.1.1 U.S. Persons Restricted Access. The AWS GovCloud (US) region is the only AWS region that has physical and logical access controls that limit access to the AWS Network by AWS personnel to U.S. Persons. Customer represents and warrants that it will only access the AWS GovCloud (US) region if: (i) Customer is a U.S. Person; (ii) Customer, if required by the International Traffic In Arms Regulations ("ITAR"), has and will maintain a valid Directorate of Defense Trade Controls registration; (iii) Customer is not subject to export restrictions under U.S. export control laws and regulations (e.g. Customer is not a denied or debarred party or otherwise subject to sanctions); and (iv) Customer maintains an effective compliance program to ensure compliance with applicable U.S. export control laws and regulations, including the ITAR. If requested by AWS, Customer agrees to provide AWS with additional documentation and cooperation to verify the accuracy of the representations and warranties set forth in this Section.

   3.1.2 Customer Responsibilities. Customer is responsible for all physical and logical access controls beyond the AWS Network including, but not limited to, Customer account access, data transmission, encryption, and appropriate storage and processing of data within the AWS GovCloud (US) region. Customer is responsible for verifying that all End Users accessing Customer Content in the AWS GovCloud (US) region are eligible to gain access to Customer Content. The Services may not be used to process or store classified data. If Customer introduces classified data into the AWS Network, Customer will be responsible for all sanitization costs incurred by AWS. Customer's liability under this provision is exempt from any limitations of liability.

3. **Definitions.**

   The following definitions are added to Section 13:

"**AWS Security Standards**" means the security standards attached to this Agreement as Attachment B.

The definition of "End User" is deleted in its entirety and replaced with the following:

"**End User**" means any entity, person, United States Federal, State or Local Government agency that directly or indirectly through another user: (a) accesses or uses Customer Content; or (b) otherwise accesses or uses the Service Offerings under a Customer account. The term "End User" does not include individuals or entities when they are accessing or using the Services or any Content under their own account, rather than a Customer account.

4. **Nondisclosure.** The contents of this Amendment are not publicly known, constitute confidential information of the parties and will not be disclosed by Customer except as required by applicable law. If a request is made for disclosure of the Agreement or this Amendment by Customer, then Customer will use commercially reasonable efforts to give AWS notice prior to disclosure.

5. **Entire Agreement; Conflict.** Except as amended by this Amendment, the Agreement will remain in full force and effect. This Amendment, together with the Agreement as amended by this Amendment: (a) is intended by the parties as a final, complete and exclusive expression of the terms of their agreement, and (b) supersedes all prior agreements and understandings between the parties with respect to the subject matter hereof. If there is a conflict between the Agreement, this Amendment or any other amendment or addendum to the Agreement or this Amendment, the document later in time will prevail.

6. **Counterparts and Facsimile Delivery.** This Amendment may be executed in two or more counterparts, each of which shall be deemed an original and all of which taken together shall be deemed to constitute one and the same document. The parties may sign and deliver this Amendment by facsimile transmission.

[Remainder of Page Intentionally Left Blank.]

ATTACHMENT B
AWS Security Standards

Capitalized terms not otherwise defined in this document have the meanings assigned to them in the applicable AWS Enterprise Customer Agreement.

1. **Information Security Program.** AWS will maintain an information security program (including the adoption and enforcement of internal policies and procedures) designed to (a) satisfy the Security Objectives, (b) identify reasonably foreseeable internal risks to security and unauthorized access to the AWS Network, and (c) minimize security risks, including through risk assessment and regular testing. AWS will designate one or more employees to coordinate and be accountable for the information security program. The information security program for the Services indicated as FISMA compliant will include the in-scope baseline security controls outlined in the NIST Special Publication ("SP") 800-53 Rev 3 for a FISMA Moderate system. The information security program for the AWS GovCloud (US) region will include internal policies, procedures and training that implement physical and logical access controls limiting access to the AWS Network for that region to U.S. Persons only. The information security program for all Services will meet the following measures:

   1.1 **Network Security.** The AWS Network will be electronically accessible to employees, contractors and any other person as necessary to provide the Services. AWS will maintain access controls and policies to manage what access is allowed to the AWS Network from each network connection and user, including the use of firewalls or functionally equivalent technology and authentication controls. AWS will maintain corrective action and incident response plans to respond to potential security threats.

   1.1.1 Network Security for AWS GovCloud (US). In addition to the security standards set forth in Section 1.1, AWS will not replicate or transmit Customer Content hosted, processed, and/or stored in the AWS GovCloud (US) region outside of the United States. AWS limits logical access to the AWS Network for the AWS GovCloud (US) region to authorized U.S. Persons by controlling access credentials, segregating the AWS GovCloud (US) region from other AWS systems, and prohibiting access to the AWS GovCloud (US) region by AWS personnel from points outside of the United States.

   1.2 **Physical Security**

   1.2.1 Physical Access Controls. Physical components of the AWS Network are housed in nondescript facilities (the "**Facilities**"). Physical barrier controls are used to prevent unauthorized entrance to the Facilities both at the perimeter and at building access points. Passage through the physical barriers at the Facilities requires either electronic access control validation (e.g., card access systems, etc.) or validation by human security personnel (e.g., contract or in-house security guard service, receptionist, etc.). Employees and contractors are assigned photo-ID badges that must be worn while the employees and contractors are at any of the Facilities. Visitors are required to sign-in with designated personnel, must show appropriate identification, are assigned a visitor ID badge that must be worn while the visitor is at any of the Facilities, and are continually escorted by authorized employees or contractors while visiting the Facilities.

   1.2.2 Limited Employee and Contractor Access. AWS provides access to the Facilities to those employees and contractors who have a legitimate business need for such access privileges. When an employee or contractor no longer has a business need for the access privileges assigned to him/her, the access privileges are promptly revoked, even if the employee or contractor continues to be an employee of AWS or its affiliates.

   1.2.3 Physical Security Protections. All access points (other than main entry doors) are maintained in a secured (locked) state. Access points to the Facilities are monitored by video surveillance cameras designed to record all individuals accessing the Facilities. AWS also maintains electronic intrusion detection systems designed to detect unauthorized access to the Facilities, including monitoring points of vulnerability with door contacts, glass breakage devices, interior motion-detection, or other

devices designed to detect individuals attempting to gain access to the Facilities. All physical access to the Facilities by employees and contractors is logged and routinely audited.

1.2.4 Pre-Employment Screening. AWS conducts criminal background checks, as permitted by applicable law, as part of pre-employment screening practices for employees and contractors commensurate with the employee's or contractor's position and level of access to the Facilities. AWS will not permit an employee or contractor to have access to the non-public Customer Content or perform material aspects of the Services if such employee or contractor has failed to pass such background check.

1.2.5 AWS GovCloud (US) Physical Access Controls. All AWS GovCloud (US) region servers are located in the United States. Access to these machines is limited to U.S. Persons. Foreign nationals, as defined by 22 CFR part 120.16, including employees, contractors, and visitors, are not permitted in controlled areas unless properly escorted at all times.

2. **Continued Evaluation.** For the Services identified as FISMA compliant, AWS in conjunction with 3rd party independent auditors will conduct annual reviews of the security of its AWS Network and adequacy of its information security program as measured against the NIST SP 800-53 security controls. AWS will conduct periodic reviews of the security of the AWS Network and adequacy of its information security program applicable to all Services as measured against industry security standards as determined by AWS and its policies and procedures. AWS will conduct periodic audits of the physical and logical access controls for the AWS GovCloud (US) region to verify the adequacy of its information security program for the region. AWS will continually evaluate the security of the AWS Network and associated Services to determine whether additional or different security measures are required to respond to new security risks or findings generated by the periodic reviews.

3. **Security Breach Notification.** If AWS has actual knowledge of a confirmed breach of the security measures described in these AWS Security Standards that affects the security of any Customer Content that is subject to applicable data breach notification law, AWS will (a) promptly notify the Customer, as required by applicable law, and (b) take commercially reasonable measures to address the breach in a timely manner. The term "breach of security" means the unauthorized access to or acquisition of any record containing Customer Content in a manner that renders misuse of the information reasonably possible.

IN WITNESS WHEREOF, Customer and AWS have executed this Amendment as of the Amendment Effective Date.

AMAZON WEB SERVICES, INC.

By: _____

Name: MAX PETERSON

Title: AWS VICE PRESIDENT

Date: 10/4/13

REGENTS OF THE UNIVERSITY OF MICHIGAN

By: _____

Name: TED EISENHUT

Title: COMMODITY MANAGER

Date: 10/11/2013