DATA PROTECTION EXHIBIT

"Data Protection Exhibit"

1. SCOPE

a. This Data Protection Exhibit outlines the terms and conditions with which the Supplier, as defined in the Glossary, must comply under any applicable Agreement it forms with Cisco which involves Processing Personal Data, or if Supplier has access to Personal Data in the course of its Performance under the Agreement. In the event of a conflict between the Agreement and this Data Protection Exhibit, the more stringent terms will apply. All capitalized terms not defined in the Glossary have the meanings set forth in the Agreement.

b. This Data Protection Exhibit includes the following appendices, which are hereby incorporated by reference:

Attachment A	BUSINESS ASSOCIATE AGREEMENT
Attachment B	STANDARD CONTRACTUAL CLAUSES
Attachment C	SUPPLIER SECURITY EXHIBIT

2. DEFAULT STANDARDS

a. To the extent that Supplier Processes Special Categories of Data, the security measures referred to in this Data Protection Exhibit shall also include, at a minimum (i) routine risk assessments of Supplier's information security program, (ii) regular testing and monitoring to measure and confirm the effectiveness of the information security program's key controls, systems, and procedures, and (iii) encryption of Special Categories of Data while "at rest" and during transmission (whether sent by e-mail, fax, or otherwise), and storage (including when stored on mobile devices, such as a portable computer, flash drive, PDA, or cellular telephone). If encryption is not feasible for mobile devices, Supplier shall store no Special Categories of Data on any mobile devices used as part of providing the Services. Further, Supplier shall protect all Special Categories of Data stored on electronic databases, servers, or other forms of non-mobile devices against all reasonably anticipated forms of compromise by use of the safeguards contained in Attachment C.

b. In addition to the foregoing, to the extent Supplier receives, processes, transmits or stores any Cardholder Data for or on behalf of Cisco, Supplier represents and warrants that information security procedures, processes, and systems will at all times meet or exceed all applicable information security laws, standards, rules, and requirements related to the collection, storage, processing, and transmission of payment card information, including those established by applicable governmental regulatory agencies, the Payment Card Industry (the "**PCI**"), all applicable networks, and any written standards provided by Cisco's information security group to Supplier from time to time (all the foregoing collectively the "**PCI Compliance Standards**").

c. Where Supplier Processes Protected Health Information (as that term is defined by The Health Insurance Portability and Accountability Act, or HIPAA), Attachment A, Business Associate Agreement will also apply to the Processing of such data.

d. If any of the Applicable Laws are superseded by new or modified Applicable Laws (including any decisions or interpretations by a relevant court or governmental authority relating thereto), the new or modified Applicable Laws shall be deemed to be incorporated into this Data Protection Exhibit, and Supplier will promptly begin complying with such Applicable Laws.

e. If this Data Protection Exhibit does not specifically address a particular data security or privacy

standard or obligation, Supplier will use appropriate, Generally Accepted Privacy Practices to protect the confidentiality, security, privacy, integrity, availability, and accuracy of Personal Data.

f. Supplier agrees that, in the event of a breach of this Data Protection Exhibit, neither Cisco nor any relevant Cisco customer will have an adequate remedy in damages and therefore either Cisco or an affected customer shall be entitled to seek injunctive or equitable relief to immediately cease or prevent the use or disclosure of Personal Data not contemplated by the Agreement and to enforce the terms of this Data Protection Exhibit or ensure compliance with all Applicable Laws.

g. Any ambiguity in this Data Protection Exhibit shall be resolved to permit Cisco to comply with all Applicable Laws. In the event and to the extent that the Applicable Laws impose stricter obligations on the Supplier than under this Data Protection Exhibit, the Applicable Laws shall prevail.

3. CERTIFICATIONS

a. Supplier must maintain the certifications listed in the Agreement, if any, and any applicable Statement of Work ("**SOW**") and Supplier shall provide annual, written, updates recertifying such certifications. If there is a material change in the requirements of a required certification or the nature of the Performance Supplier is providing, such that Supplier no longer wishes to maintain such certifications, Supplier will request such changes in writing to Cisco and the parties will discuss alternatives and compensating controls in good faith. Such change would allow Cisco to terminate any underlying Agreement(s) for cause and without penalty to Cisco.

b. Prior to Processing Personal Data, Supplier will provide Cisco with copies of any certifications it maintains (along with relevant supporting documentation) that apply to the systems, policies, and procedures that govern the Processing of Personal Data. Supplier will promptly notify Cisco if Supplier has failed or no longer intends to adhere to such certifications or successor frameworks. Examples of potentially relevant certifications include: SSAE 16 – SOC1, SOC2, SOC3; ISO 27001:2013; ISO 27018:2014, EU Binding Corporate Rules; APEC Cross Border Privacy Rules System; EU-US and Swiss-US Privacy Shields; Payment Card Industry Data Security Standards (PCI-DSS); and Federal Information Security Management Act (FISMA) Compliance Certification.

c. If Supplier does not maintain any external certifications related to privacy, security, or data protection associated with Supplier's Processing of Personal Data:

   i. Supplier shall provide Cisco with documentation requested by Cisco sufficient to demonstrate Supplier is in compliance with Section 4 of this Data Protection Exhibit and the technical and organizational security measures outlined in Attachment C.

   ii. Cisco and/or its duly authorized representatives, or in the case of a Cisco customer, the customer and/or its duly authorized representatives, shall have the right to conduct its own security audit of Supplier in the event of reasonable suspicion or identification of any inadequately mitigated material security related risk related to Cisco, Personal Data, or systems. Such audit shall be conducted with reasonable advanced notice to Supplier, and shall take place during normal business hours to reasonably limit disruption to Supplier's business.

d. Cisco shall treat the contents of and reports related to Supplier's security and certifications as Confidential Information pursuant to the terms contained in the Agreement between the parties.

4. DATA PROTECTION AND PRIVACY

a. If Supplier has access to or otherwise Processes Personal Data, then Supplier shall:

i. implement and maintain commercially reasonable and appropriate physical, technical, and organizational security measures described in this Data Protection Exhibit (including any appendices or attachments or referenced certifications) to protect Personal Data against accidental or unlawful destruction; accidental loss, alteration, unauthorized disclosure or access; all other unlawful forms of Processing; and any Information Security Breach, as defined in Attachment C;

ii. take reasonable steps to ensure the reliability of its staff and any other person acting under its supervision who may come into contact with, or otherwise have access to and Process Personal Data; and ensure that such personnel are aware of their responsibilities under this Data Protection Exhibit and any Applicable Law (or Supplier's own written binding policies that are at least as restrictive as this Data Protection Exhibit);

iii. assist Cisco as needed to respond to requests from supervisor authorities, data subjects, customers, or others to provide information (including details of the Services provided by Supplier) related to Supplier's Processing of Personal Data;

iv. not (1) transfer Personal Data from the EEA or Switzerland to, or (2) access, disclose, Process Personal Data from the EEA or Switzerland in, a jurisdiction which is not an Approved Jurisdiction, nor require Cisco or a customer of Cisco to do so, unless it first obtains Cisco's advance written consent and require any sub-contractor to agree to terms consistent with this Data Protection Exhibit (and in which case, Section 5, below, will apply);

Where Supplier processes Personal Data from the EEA or Switzerland on behalf of Cisco, Supplier shall perform such processing in a manner consistent with the Privacy Shield Principles (see www.commerce.gov/privacyshield) or its successor framework(s) to the extent the Principles are applicable to Supplier's processing of such data. If Supplier is unable to provide the same level of protection as required by the Principles, Supplier shall immediately notify Cisco and cease processing. Any non-compliance with the Principles shall be deemed a material breach of the Agreement and Cisco shall have the right to terminate the Agreement immediately without penalty.

v. for jurisdictions other than the EEA or Switzerland, not transfer Personal Data outside of a particular jurisdiction unless permitted under Applicable Laws; and meet all security and privacy standards to allow such transfer.

Where Supplier processes Personal Data from the APEC Member Economies on behalf of Cisco, Supplier shall perform such processing in a manner consistent with the APEC Cross Border Privacy Rules Systems requirements ("**CBPRs**") (see www.cbprs.org) to the extent the requirements are applicable to Supplier's Processing of such data. If Supplier is unable to provide the same level of protection as required by the CBPRs, Supplier shall immediately notify Cisco and cease processing. Any non-compliance with the CBPRs shall be deemed a material breach of the Agreement and Cisco shall have the right to terminate the Agreement immediately without penalty.

b. In addition, if Supplier Processes Personal Data in the course of Performance under the Agreement or a SOW, then Supplier shall also:

i. only Process the Personal Data in accordance with Cisco instructions, the Agreement, and this Data Protection Exhibit, but only to the extent that such instructions are consistent with Applicable Law. If Supplier reasonably believes that Cisco's instructions are inconsistent

with Applicable Law, Supplier will promptly notify Cisco of such;

ii. only process or use Personal Data on its systems or facilities to the extent necessary to Perform its obligations under the Agreement, or an applicable SOW solely on behalf of Cisco and only for the purposes provided under the Agreement, or an applicable SOW;

iii. where applicable, act as a subprocessor of such Personal Data;

iv. maintain accurate records of the Processing of any Personal Data received from Cisco under the Agreement;

v. make reasonable efforts to ensure that Personal Data are accurate and up to date at all times while in its custody or under its control, to the extent Supplier has the ability to do so;

vi. not lease, sell, distribute, or otherwise encumber Personal Data (including in aggregated form) unless mutually agreed to by separate signed, written agreement;

vii. provide full, reasonable cooperation and assistance to Cisco in allowing the persons to whom Personal Data relate to have access to those data and to delete or correct such Personal Data if they are demonstrably incorrect (or, if Cisco or Cisco's customer does not agree that they are incorrect, to have recorded the fact that the relevant person considers the data to be incorrect);

viii. provide such assistance as Cisco or its customer reasonably requests and Supplier or a Contractor is reasonably able to provide with a view to meeting any applicable filing, approval or similar requirements in relation to Applicable Laws;

ix. promptly notify Cisco at: data-incident-command@cisco.com of any investigation, litigation, arbitrated matter or other dispute relating to Supplier's information security or privacy practices as it relates to the Performance, Supplier provides to Cisco;

x. promptly notify Cisco in writing and provide Cisco an opportunity to intervene in any judicial or administrative process if Supplier is required by law, court order, warrant, subpoena, or other legal or judicial process to disclose any Personal Data to any person other than Cisco, or a Cisco subcontractor expressly approved by Cisco, or the relevant Cisco customer to receive such information; and

xi. on termination of the Agreement for whatever reason, or upon written request at any time during the Term, Supplier shall cease to Process any Personal Data received from Cisco, and within a reasonable period will, at the request of Cisco: 1) return all Personal Data; or 2) securely and completely destroy or erase (using a standard such as US Department of Defense 5220.22-M or British HMG Infosec Standard 5, Enhanced Standard) all Personal Data in its possession or control. At Cisco's request, Supplier shall give Cisco a certificate signed by one of its senior managers, confirming that it has fully complied with this Clause.

5. INDEMNIFICATION

Supplier agrees to indemnify and hold harmless Cisco and its affiliates, directors, officers, employees, and agents (other than Supplier), individually and collectively, against any and all losses, liabilities, judgments, penalties, awards and costs, including costs of investigation and legal fees and expenses, arising out of or related to: (i) a breach of any representation, warranty, or covenant of this Data Protection Exhibit; or (ii) any negligent or wrongful acts or omissions of Supplier or its Representatives. This section is intended to control all indemnification situations between the parties with respect to (i) and (ii) above, including breaches, and no limitations of liability, or any exclusions contained in a consequential damages provision, or indemnification provisions in any other agreements between

Cisco and Supplier shall be applicable to this Data Protection Exhibit to relieve Supplier of its indemnification obligations hereunder. For the avoidance of doubt, this includes Supplier liability for and duty to indemnify Cisco against any and all claims, actions, liabilities, losses, damages and expenses (including legal expenses) incurred by Cisco which arise directly or indirectly out of or in connection with Supplier's data processing activities under this Agreement including without limitation those arising out of any third party demand, claim or action, or any breach of contract, negligence, fraud, willful misconduct, breach of statutory duty or non-compliance with any Applicable Laws by Supplier or its employees, agents or contractors. This section is intended to survive any expiration or termination of the Agreement.

6. STANDARD CONTRACTURAL CLAUSES FOR THE PROCESSING OF PERSONAL DATA

If, and only with Cisco's prior consent, Supplier Processes Personal Data from the EEA or Switzerland in a jurisdiction that is not an Approved Jurisdiction, Supplier shall ensure that it has a legally approved mechanism in place to allow for the international data transfer. If Supplier intends to rely on Standard Contractual Clauses, the following additional terms will apply to Supplier and Supplier's subcontractors and/or affiliates (where subcontracting or Performance is allowed by the Agreement):

a. The Standard Contractual Clauses set forth in Attachment B will apply. If such Standard Contractual Clauses are superseded by new or modified Standard Contractual Clauses, the new or modified Standard Contractual Clauses shall be deemed to be incorporated into this Data Protection Exhibit, will replace the then-current Attachment B, and Supplier will promptly begin complying with such Standard Contractual Clauses. Supplier will abide by the obligations set forth under the Standard Contractual Clauses for data importer and/or subprocessor as the case may be.

b. If Supplier subcontracts any Processing of Personal Data (if expressly allowed by the Agreement and Applicable Law), it will:

   i. Notify Cisco in advance of such processing and obtain Cisco's written permission before proceeding; and

   ii. Ensure that Supplier's Contractors have entered into the Standard Contractual Clauses with Supplier or another agreement in which the Contractors agree to abide by Clause 5 of the Standard Contractual Clauses with respect to such Personal Data and which complies with Clauses 3(3), 6(3) and 11 of the Standard Contractual Clauses.

c. Where reasonably requested by Cisco's customers via Cisco, Supplier will enter into the Standard Contractual Clauses directly with such customers.

7. SUBCONTRACTING

a. Supplier shall have a documented security program and policies that provide guidance to its Contractors to ensure the security, confidentiality, integrity, and availability of personal data and systems maintained or processed by Supplier, and that provides express instructions regarding the steps to take in the event of a compromise or other anomalous event.

b. Supplier shall not subcontract its obligations under this Data Protection Exhibit to another person or entity, in whole or in part, without Cisco's prior written approval. Prior to seeking Cisco's consent, Supplier shall provide Cisco with full details of the proposed Contractor's involvement including the identity of the Contractor, its data security record, the location of its processing facilities, a description of the access to Personal Data proposed, and any other information Cisco may reasonably request in order to assess the risks involved in allowing the Contractor to process Personal Data.

c. Supplier will execute a written agreement with such approved Contractor containing equivalent terms to this Data Protection Exhibit and the applicable Exhibits (provided that Supplier shall not be entitled to permit the Contractor to further sub-contract or otherwise delegate all or any part of the Contractor's processing without Supplier's prior written consent) and which provides Cisco with third party beneficiary rights to enforce such terms; and/or require Supplier to procure that the Contractor enters into a Data Protection agreement with Cisco directly if privity of contract is required by law.

d. Supplier shall be responsible and accountable for the acts or omissions of Representatives to the same extent it is responsible and accountable for its own actions or omissions under this Data Protection Exhibit.

ATTACHMENT A
BUSINESS ASSOCIATE AGREEMENT

For purposes of this Business Associate Agreement Attachment, the Supplier shall be hereinafter referred to as "Business Associate".

RECITALS

WHEREAS, Subtitle F of the Health Insurance Portability and Accountability Act of 1996, Public Law No. 104-191, as amended by the American Recovery and Reinvestment Act of 2009, Public Law No. 111-005, Part I, Title XIII, Subpart D, Sections 13401-13409, (the "HITECH Act"), (collectively, "HIPAA") provides that Cisco comply with standards to protect the security, confidentiality and integrity of health information; and

WHEREAS, the Department of Health and Human Services has issued regulations under HIPAA (the "HIPAA Regulations"), including the Standards for Privacy of Individually Identifiable Health Information, 45 CFR Parts 160 and 164, sub-parts A and E, as amended by the HITECH Act (the "Privacy Rule") and the Standards for Security of Electronic Protected Health Information, 45 CFR Parts 160, 162 and 164, as amended by the HITECH Act (the "Security Rule") (collectively, the "Privacy and Security Rules"); and

WHEREAS, Sections 164.502(e) and 164.504(e) of the Privacy and Security Rules set forth standards and requirements for Cisco to enter into written agreements with certain business associates that will have access to Cisco's Protected Health Information (as defined below); and

WHEREAS, Business Associate will provide services under the Agreement as a subcontractor to Cisco on behalf of a Covered Entity (as defined in the Privacy and Security Rules).

NOW THEREFORE, in consideration of the mutual promises below, the parties agree as follows:

1. Definitions

1.1. "Breach" shall have the meaning given to such term in 45 CFR Section 164.402.

1.2. "Designated Record Set" shall have the meaning given to such term under the Privacy Rule at 45 CFR Section 164.501.

1.3. "Electronic Protected Health Information" or "Electronic PHI" shall mean Protected Health Information which is transmitted by Electronic Media (as defined in the Privacy and Security Rules) or maintained in Electronic Media.

1.4. "Individual" shall have the meaning given to such term under the Privacy and Security Rules at 45 CFR Section 164.103 and shall include a person who qualifies as a personal representative in accordance with 45 CFR Section 164.502(g).

1.5. "Protected Health Information" or "PHI" shall have the meaning given to such term under the Privacy and Security Rules at 45 CFR Section 164.103, limited to the information created or received by Business Associate from or on behalf of Cisco. "Protected Health Information" includes, without limitation, "Electronic Protected Health Information".

1.6. "Required by Law" shall have the meaning given to such term under the Privacy and Security Rules at 45 CFR Section 164.103.

1.7. "Secretary" shall mean the Secretary of the Department of Health and Human Services or his or her designee.

1.8. "Security Incident" shall have the meaning given to such term under the Security Rule at 45 CFR Section 164.304.

2. Permitted Uses and Disclosures of PHI. Business Associate agrees not to use or further disclose PHI other than as permitted or required by this Attachment or as otherwise Required By Law. In connection with the foregoing and except as otherwise limited in this Attachment, Business Associate may:

2.1. Use or disclose PHI to perform functions, activities or services for, or on behalf of, Cisco that are necessary to Perform under the Agreement or applicable SOW, provided that such use or disclosure would not violate the Privacy and Security Rules if done by Cisco;

2.2. Use PHI for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate; and

2.3. Disclose PHI for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate, provided (i) the disclosure is Required by Law, or (ii) Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and will be used or further disclosed only as Required by Law or for the purpose for which it was disclosed to the person, and that the person agrees to notify Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

3. Responsibilities of Business Associate.

3.1. Appropriate Safeguards. Business Associate shall use appropriate safeguards to prevent use or disclosure of PHI other than as provided for by the Attachment. Business Associate shall implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of Electronic PHI, as required by the Security Rule. In furtherance of compliance with such requirements, Business Associate shall:

3.1.1. maintain an information security program that meets or exceeds the level required by the HIPAA Security Rule;

3.1.2. maintain policies and procedures for Business Associate's organization, consistent with the HIPAA Privacy and Security Rules and must identify an individual within the Business Associate's organization who is responsible for enforcement and oversight of such privacy and security policies and procedures;

3.1.3. ensure that any and all employees of Business Associate that handle or access PHI must undergo ongoing training regarding the safeguarding of PHI;

3.1.4. ensure that any and all third parties that access Covered Entity's confidential data or PHI with whom Business Associate contracts with or relies upon for the provision of services also maintain a framework for compliance with the HIPAA Privacy and Security Rules;

3.1.5. implement a contingency plan for responding to emergencies and/or disruptions to business that in any way affect the use, access, disclosure or other handling of Covered Entity's data and PHI;

3.1.6. maintain and exercise a plan to respond to internal and external security threats and violations, including an incident response plan;

3.1.7. maintain policies and procedures that specifically address how security breaches that are identified will be addressed;

3.1.8. maintain technology policies and procedures that provide reasonable safeguards for the protection of PHI on hardware and software utilized by Business Associate;

3.1.9. ensure that for the electronic transmission of PHI is encrypted meeting at least the minimum standards required by Cisco's data security policies and applicable National Institute of Standards and Technology guidelines.

3.2. Security Survey. During the term of this Attachment, Business Associate may be asked to complete a security survey and/or attestation document designed to assist Cisco in understanding and documenting Business Associate's security procedures and compliance with the requirements contained herein. Business Associate's failure to complete either of these documents within the reasonable timeframe specified by Cisco shall constitute a material breach of the Agreement.

3.3. Additional Information. Business Associate shall provide Cisco with information concerning the aforementioned safeguards and/or other information security practices as they pertain to the protection of Covered Entity's PHI, as Cisco may from time to time request. Failure of Business Associate to complete or to respond to Cisco's request for information within the reasonable timeframe specified by Cisco shall constitute a material breach of the Agreement. If Cisco has reasonable concern regarding compliance with the terms of this Attachment or the occurrence of a breach, Cisco will be granted access to facilities in order to review policies, procedures and controls relating to the compliance with the terms of this Attachment.

3.4. Reporting of Improper Use or Disclosure. Business Associate shall promptly report to Cisco any use or disclosure of PHI not provided for by the Attachment of which it becomes aware, including breaches of Unsecured Protected Health Information (as defined in the Privacy and Security Rules). In addition, Business Associate shall promptly report to Cisco any Security Incident. If Cisco determines that such use or disclosure may constitute a Breach of Unsecured Protected Health Information, Business Associate agrees to provide Cisco written notification of the Breach that includes the following information within three (3) days: (1) a brief description of the incident, including the date of the Breach and the date of the discovery of the Breach; (2) the identification of each individual whose Unsecured PHI was breached; (3) a description of the types of Unsecured PHI that were involved in the Breach; (4) any steps individuals should take to protect themselves from potential harm resulting from the Breach; and (5) a brief description of actions that Business Associate is undertaking to investigate the Breach, to mitigate harm to individuals, and to protect against any further breaches.

3.5. Business Associate's Agents. Business Associate shall ensure that any agent, including a subcontractor, to whom it provides any PHI received from Cisco agrees to the same restrictions and conditions that apply through this Attachment to Business Associate with respect to such PHI.

3.6. Access to PHI. At the request of Cisco, and in the time and manner designated by Cisco, Business Associate shall make available PHI in a Designated Record set to Cisco as necessary to meet the requirements under 45 CFR Section 164.524.

3.7. Amendment of PHI. At the request of Cisco, and in the time and manner designated by Cisco, Business Associate shall make any amendment(s) to PHI maintained in a Designated Record Set pursuant to 45 CFR Section 164.526.

3.8. Documentation of Disclosures. Business Associate agrees to document such disclosures of PHI and information related to such disclosures as would be required for Cisco to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR Section 164.528. At a minimum, such information shall include: (i) the date of disclosure; (ii) the name of the entity or person who received PHI and, if known, the address of the entity or person; (iii) a brief description of the PHI disclosed; and (iv) a brief statement of the purpose of the disclosure that reasonably informs the Individual of the basis for the disclosure, or a copy of the Individual's authorization, or a copy of the written request for disclosure.

3.9. Accounting of Disclosures. Business Associate agrees to provide to Cisco, in the reasonable time and manner designated by Cisco, information collected in accordance with Section 4(f) of this Attachment, to permit Cisco to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR Section 164.528.

3.10. Governmental Access to Records. Business Associate shall make its internal practices, books and records, including policies and procedures and PHI, relating to the use and disclosure of PHI received from, or created or received by Business Associate on behalf of, Cisco available to the Secretary for purposes of the Secretary determining Cisco's compliance with the Privacy and Security Rules.

4. Responsibilities of Cisco. In addition to any other obligations set forth in this Attachment, Cisco shall:

4.1. provide to Business Associate only the minimum PHI necessary to accomplish the services;

4.2. implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of Electronic PHI, as required by the Security Rule; and

4.3. obtain any consent or authorization that may be required by applicable or federal or state laws and regulations prior to furnishing PHI to Business Associate.

5. Term and Termination. The term of this Attachment shall commence as of the Effective Date and continue coterminous with the Agreement unless otherwise terminated as set forth herein. Upon Cisco's knowledge of a material breach by Business Associate of this Attachment, Cisco shall either (i) provide an opportunity for Business Associate to cure the breach or end the violation within the time specified by Cisco, or (ii) immediately terminate this Attachment if cure is not possible. Upon termination of this Attachment for any reason, Business Associate shall return or destroy all PHI received from Cisco, or created or received by Business Associate on behalf of Cisco, and shall retain no copies of PHI. In the event that Business Associate determines that returning or destroying the PHI is infeasible, Business Associate shall provide to Cisco notification of the conditions that make return or destruction infeasible. If Business Associate determines that return or destruction of PHI is infeasible, BA shall extend the protections of this Attachment to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such PHI.

6. Regulatory References. A reference in this Attachment to a section in the Privacy and Security Rules means the section as in effect or as amended, and for which compliance is required.

7. No Agency Relationship. The parties agree that each individual party shall maintain its own independent HIPAA and HITECH Act compliance obligations. The parties will be providing their services as separate legal entities and independent contractors. The parties expressly agree that no agency relationship is created by this Attachment or the underlying Agreement with regard to the individual parties' HIPAA obligations. Each party certifies that (1) Cisco shall not have the right or authority to control Business Associate's conduct in the performance of services or in the performance of HIPAA obligations; (2) Cisco shall not have the authority to direct the daily performance of services by Business Associate; and (3) Cisco shall not have the right to give interim instruction to Business Associate regarding the performance of services.

8. Interpretation. Any ambiguity in this Attachment shall be resolved to permit Cisco to comply with the Privacy and Security Rules.

ATTACHMENT B

Standard Contractual Clauses

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection (These can be located in their original text on the European Commission website here: http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm).

For purposes of this Attachment B:

any reference to "data exporter" means Cisco, acting as data exporter on behalf of its EEA or Swiss customer(s) where applicable,

and

any reference to "data importer" means Supplier

each a "**party**"; together "**the parties**".

The parties have agreed on the following Standard Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or

access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission

of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data controller is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain

fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data controller is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

APPENDIX 1 TO ATTACHMENT B

THE STANDARD CONTRACTUAL CLAUSES

This Appendix 1 forms part of the Clauses.

Data exporter

The data exporter is Cisco, acting as data exporter on behalf of itself or a customer where applicable. Activities relevant to the transfer include the performance of services for Cisco and its customer(s).

Data importer

The data importer is Supplier. Activities relevant to the transfer include the performance of services for Cisco and customers.

Data subjects

The personal data transferred may concern the following categories of data subjects: Employees, contractors, business partners, representatives and end customers of customers, and other individuals whose personal data is processed by or on behalf of Cisco or Cisco's customers and delivered as part of the Services.

Categories of data

The personal data transferred may concern the following categories of data:

Personal Data related directly or indirectly to the delivery of services or Performance, including online and offline customer, prospect, partner, and supplier data, and personal data provided by customers in connection with the resolution of support requests.

Special categories of data

The personal data transferred may concern the following special categories of data:

Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union memberships, and data concerning health or sex life, and data relating to offenses, criminal convictions or security measures.

Processing operations

The personal data transferred may be subject to the following basic processing activities, as may be further set forth in contractual agreements entered into from time to time between Cisco and customers: (a) customer service activities, such as processing orders, providing technical support and improving offerings, (b) sales and marketing activities as permissible under applicable law, (c) consulting, professional, security, storage, hosting and other services delivered to customers, including services offered by means of the products and solutions described at www.cisco.com, and (d) internal business processes and management, fraud detection and prevention, and compliance with governmental, legislative, and regulatory requirements.

ATTACHMENT C

SUPPLIER SECURITY EXHIBIT

(Also known as APPENDIX 2 TO ATTACHMENT B STANDARD CONTRACTUAL CLAUSES)

Scope:

The Supplier Security Exhibit provides details of the information security expectations and conduct between Cisco and Supplier and is available online at http://www-author.cisco.com/c/dam/en_us/about/doing_business/legal/docs/supplier-security-exhibit.pdf.

Supplier acknowledges and agrees that the Supplier Security Exhibit is applicable to its Performance under the Agreement pursuant to this Data Protection Exhibit, and forms a part of this Data Protection Exhibit by this reference. References to Supplier in the Supplier Security Exhibit shall also mean the 'data importer'. By executing the Agreement, the Supplier represents, warrants, and confirms that it has reviewed the Supplier Security Exhibit and is bound by all the terms and conditions contained therein.