SUPPLIER PRIVACY AND INFORMATION SECURITY EXHIBIT

1. SCOPE

a. This Data Protection Exhibit outlines the terms and conditions with which the Supplier 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
Attachment D	GLOSSARY

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. 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.

6. 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)

1. Scope

This SSE outlines the information security expectations and requirements between Cisco and Supplier and describes the technical and organizational security measures that must be implemented by the Supplier to secure Protected Data prior to the Performance of any part of the Agreement.

All capitalized terms not defined in the Glossary have the meanings set forth in the Agreement.

2. General Security Practices

a. Supplier has implemented and shall maintain appropriate technical and organizational measures to protect Protected Data against accidental loss, destruction or alteration, unauthorized disclosure or access, or unlawful destruction, including the policies, procedures, and internal controls set forth in this SSE for its personnel, equipment, and facilities at the Supplier's locations involved in Performing any part of the Agreement with Cisco.

3. General Compliance

a. **Compliance**. The Supplier shall document and implement processes and procedures to avoid breaches of legal, statutory, regulatory, or contractual obligations related to information security and of any security requirements. Such processes and procedures shall be designed to provide appropriate security to protect Protected Data given the risk posed by the nature of the data Processed by Supplier. The Supplier shall ensure that information security is implemented and operated in accordance with the Supplier's organizational policies and procedures.

b. **Intellectual property rights**. Supplier shall implement appropriate procedures to ensure compliance with legislative, regulatory, and contractual requirements related to Intellectual Property Rights and use of proprietary software products.

c. **Protection of records**. Supplier shall protect records from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislative, regulatory, contractual, and business requirements.

d. **Independent review of information security.** Supplier's approach to managing information security and its implementation (i.e., control objectives, controls, policies, processes, and procedures for information security) shall be reviewed independently at planned intervals or when significant changes occur.

e. **Compliance with security policies and standards.** Supplier's management shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards, and any other security requirements.

f. **Technical compliance review.** Supplier's information systems shall be regularly reviewed for compliance with the organization's information security policies and standards.

g. **Information Risk Management ("IRM").** Risk assessment is the process of assessing potential business impact, evaluating threats and vulnerabilities, and selecting appropriate controls to meet the business requirements for information security. Supplier is required to have a risk management framework and conduct a yearly risk assessment of their environment and systems to understand their risks and apply appropriate

controls to manage and mitigate the risks. Threat and vulnerability assessment must be periodically reviewed and remediation actions taken where material weaknesses are found. Supplier will provide Cisco with the reports and analysis upon written request, provided the disclosure of which would not violate Supplier's own information security policies, or Applicable Laws.

4. Technical and Organizational Measures for Security

a. **Organization of Information Security**

i. **Security Ownership**. Supplier shall appoint one or more security officers responsible for coordinating and monitoring the security rules and procedures. Such officers shall have the knowledge, experience, and authority to serve as the owner(s), with responsibility and accountability for information security within the organization.

ii. **Security Roles and Responsibilities**. Supplier shall ensure that all information security responsibilities are defined and allocated in accordance with Supplier's approved policies for information security. Such policies shall be published and communicated to employees and relevant external parties.

iii. **Project Management.** Supplier shall ensure that information security be addressed in project management, regardless of the type of project to ensure that information security risks are identified and addressed as part of the project.

iv. **Risk Management**. Supplier shall have a risk management framework and conduct a yearly risk assessment of its environment and systems to understand its risks and apply appropriate controls to manage and mitigate risks before processing Protected Data or offering its services.

b. **Human Resources Security**

i. **General**. Supplier shall inform its personnel about relevant security procedures and their roles and ensure that personnel with access to Protected Data are subject to written confidentiality obligations. Supplier shall further inform its personnel of possible consequences of breaching Supplier's security policies and procedures, which must include disciplinary action, including termination of employment for Supplier's employees and termination of contract or assignment for Contractors and temporary personnel.

ii. **Training**. Supplier personnel with access to Protected Data shall receive annual education and training regarding privacy and security procedures for services to aid in the prevention of unauthorized use (or inadvertent disclosure) of Protected Data and training regarding how to effectively respond to security incidents.

1. Training shall be provided before Supplier personnel have access to Protected Data or begin providing services.

2. Training shall be regularly reinforced through refresher training courses, emails, posters, notice boards, and other training and awareness materials.

iii. **Background Checks**. In addition to any other terms in the Agreement related to this subject matter, Supplier shall perform criminal and other relevant background checks on its personnel in compliance with local laws.

c. **Asset Management**

i. **Asset Inventory**. Access to Protected Data shall be restricted to Supplier personnel authorized in writing to have such access.

ii. **Information Classification**. Supplier shall classify, categorize, and/or tag Protected Data to help identify it and to allow for access to it to be appropriately restricted.

iii. **Trusted Device Standards.**

Supplier personnel shall:

1. Use trusted devices that are configured with security software (i.e., anti-virus, anti-malware, encryption, etc.) and protected against corruption, loss, or disclosure;

2. Follow Cisco's trusted device standards when accessing Protected Data or when having Protected Data in his/her control. The trusted device standard specifies the requirements that user devices ("**devices**") must satisfy to be trusted when processing Protected Data whether or not connected to a Cisco network through wired, wireless, or remote access (the "**network**"). Devices that fail to comply with this standard will not be entitled to access to the network unless Cisco determines limited access is acceptable. Cisco's network access policies establish requirements for physical and wireless network data ports that provide local network communications and telephony services.

   Cisco's trusted device standards include, at a minimum, the following requirements:

   A. Each device must be uniquely associated with a specific, individual user;

   B. Devices must be configured for automatic patching. All OS and application security patches must be installed within four (4) weeks of release. Devices may be required to immediately install emergency patches as necessary;

   C. Devices must be encrypted (i.e., full disk, endpoint encryption) and secured with a password/PIN screen lock with the automatic activation feature set to ten (10) minutes or less. Users must lock the screen or log off when the device is unattended;

   D. Devices must not be rooted or jailbroken;

   E. Devices must be periodically scanned for restricted or prohibited software (e.g., peer-to-peer sharing and social media apps); and

   F. Devices must run an acceptable industry standard anti-malware solution. On-access scan and automatic update functionality must be enabled.

3. Not accept or store Protected Data on smartphones, tablets, USB drives, DVD/CDs, or other portable media without prior written authorization from Cisco; and

4. Take measures to prevent accidental exposure of Protected Data (e.g. using privacy filters on laptops when in areas where over-the-shoulder viewing of Protected Data is possible).

iv. **Personnel Access Controls**

1. **Access.**

   A. Limited Use. Supplier understands and acknowledges that Cisco and Cisco's customers may be providing access to sensitive and proprietary information and access to computer systems to Supplier in order to Perform under the Agreement. Supplier represents and warrants that it will not access the Protected Data or computer systems for any purpose other than as necessary to Perform under the Agreement; and Supplier will not use any system access

information (such as usernames or passwords) to gain unauthorized access to Protected Data or Cisco or its customers' systems, or to exceed the scope of any authorized access.

B. Authorization. Supplier shall restrict access to Protected Data and systems at all times solely to those individual Contractors whose access is essential to Performing under the Agreement.

C. Suspension or Termination of Access Rights. At Cisco's request, Supplier shall immediately suspend or terminate the access rights to Protected Data and systems for any Supplier's personnel or its Contractors suspected of breaching any of the provisions of this SSE; and Supplier shall remove access rights of all employees and external party users upon suspension or termination of their employment, contract, or agreement.

2. **Access Policy**. Supplier shall determine appropriate access control rules, rights, and restrictions for each specific user's roles towards their assets. Supplier shall maintain a record of security privileges of its personnel that have access to Protected Data, networks, and network services. Supplier shall restrict and tightly control the use of utility programs that might be capable of overriding system and application controls.

3. **Access Authorization**.

A. Supplier shall have user account creation and deletion procedures, with appropriate approvals, for granting and revoking access to Cisco's and customers' systems and networks. Supplier shall use an enterprise access control system that requires its personnel revalidation by managers at regular intervals based on the principle of "least privilege" and need-to-know criteria based on job role.

B. Supplier shall maintain and update a record of personnel authorized to access systems that contain Protected Data and Supplier shall review users' access rights at regular intervals.

C. For systems that process Protected Data, Supplier shall revalidate 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 (6) months.

D. Supplier shall ensure that access to program source code and associated items such as software object code, designs, specifications, verification plans, and validation plans, will be restricted in order to prevent the introduction of unauthorized functionality and to avoid unintentional changes.

4. **Network Design**. For systems that process Protected Data, Supplier shall have controls to avoid personnel assuming access rights they have not been assigned to gain unauthorized access to Protected Data.

5. **Least Privilege**. Supplier shall limit access to Protected Data to those personnel Performing under the Agreement and, to the extent technical support is needed, its personnel performing such technical support.

6. **Authentication**

A. Supplier shall use industry standard practices to identify and authenticate users who attempt to access information systems. Where authentication mechanisms are based on passwords, Supplier shall require that the passwords are renewed regularly, no less often than every six (6) months.

B. Where authentication mechanisms are based on passwords, Supplier shall require the password to conform to very strong password control parameters (e.g., biometrics, multi-factor authentication, length, character complexity, and/or non-repeatability).

C. Supplier shall ensure that de-activated or expired identifiers are not granted to other individuals.

D. Supplier shall monitor repeated attempts to gain access to the information system using an invalid password.

E. Supplier shall maintain industry standard procedures to deactivate passwords that have been corrupted or inadvertently disclosed.

F. Supplier shall use 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 (e.g., passwords shall not be stored or shared in plain text). Such practices shall be designed to ensure strong, confidential passwords.

v. **Cryptography**

1. **Cryptographic controls policy**

A. Supplier shall have a policy on the use of cryptographic controls based on assessed risks.

B. Supplier shall assess and manage 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.

C. Supplier's cryptographic controls/policy shall address appropriate algorithm selections, key management and other core features of cryptographic implementations.

2. **Key management**. Supplier shall have procedures for distributing, storing, archiving, and changing/updating keys; recovering, revoking/destroying, and dealing with compromised keys; and logging all transactions associated with such keys.

vi. **Physical and Environmental Security**

1. **Physical Access to Facilities**

A. Supplier shall limit access to facilities where systems that process Protected Data are located to authorize individuals.

B. Security perimeters shall be defined and used to protect areas that contain both sensitive or critical information and information processing facilities.

C. Facilities shall be monitored and access controlled at all times (24x7).

D. Access shall be controlled through key card and/or appropriate sign-in procedures for facilities with systems processing Protected Data. Supplier must register personnel and require them to carry appropriate identification badges.

2. **Physical Access to Equipment**. Supplier equipment that is located off premises shall be protected using industry standard process to limit access to authorized individuals.

3. **Protection from Disruptions**. Supplier shall use a variety of industry standard systems to protect against loss of data due to power supply failure or line interference.

4. **Clear Desk**. Supplier shall have policies requiring a "clean desk/clear screen".

vii. **Operations Security**

1. **Operational Policy**. Supplier shall maintain written policies describing its security measures and the relevant procedures and responsibilities of its personnel who have access to Protected Data and to its systems and networks. Supplier shall ensure the policies are communicated to all persons involved in the processing of Protected Data. Compliance with such policy and all relevant legislation and regulations concerning the protection of the privacy of people and the protection of Protected Data requires appropriate management structure and control.

2. **Security and Processing Controls**.

A. **Areas**. Supplier shall maintain, document, and make available standards and procedures to address the configuration, operation, and management of systems and networks, services, and Protected Data.

B. **Standards and Procedures.** The standards and procedures shall include: security controls; identification and patching of security vulnerabilities; change control process and procedures; problem management; and incident detection and management.

3. **Logging and Monitoring**. Supplier shall maintain logs of administrator and operator activity and data recovery events.

viii. **Communications Security and Data Transfer**

1. **Networks**. Supplier shall, at a minimum, use the following controls to secure its networks that access Cisco or customer servers which store Protected Data:

A. Network traffic shall pass through firewalls, which are monitored at all times. Supplier must implement intrusion prevention systems that allow traffic flowing through the firewalls and LAN to be logged and protected at all times.

B. Access to network devices for administration must utilize a minimum of 256-bit, industry standard encryption.

C. Anti-spoofing filters must be enabled on routers.

D. 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.

E. Initial user passwords are required to be changed during the first log-on. Supplier shall have a policy prohibiting the sharing of user IDs and passwords.

F. Firewalls must be deployed to protect the perimeter of Cisco and customers' networks.

2. **Virtual Private Networks ("VPN")**. When remote connectivity to the Cisco network is required for processing of Protected Data, Supplier shall use VPN servers for the remote access with the following or similar capabilities:

A. Connections must be encrypted using a minimum of 256-bitbit encryption.

B. Connections from Cisco or its customers to Supplier locations shall only be established using the Cisco VPN servers.

C. The use of multi -factor authentication is required.

3. **Data Transfer**. Supplier shall have formal transfer policies in place to protect the transfer of information through the use of all types of communication facilities that adhere to the requirements of this SSE. Such policies shall be designed to protect transferred information from interception, copying, modification, corruption, mis-routing and destruction.

ix. **System Acquisition, Development, and Maintenance**

1. **Security Requirements**. Supplier shall adopt security requirements for the purchase, use, or development of information systems, including for application services delivered through public networks.

2. **Development Requirements**. Supplier shall have policies for secure development, system engineering, and support. Supplier shall conduct appropriate tests for system security as part of acceptance testing processes Supplier shall supervise and monitor the activity of outsourced system development.

x. **Penetration Testing and Vulnerability Scanning & Audit Reports**

1. **Testing.** Supplier will perform annual penetration test on their internet perimeter network. Audits will be conducted by the Supplier compliance team using industry recommended network security tools to identify vulnerability information. Upon request from Cisco, Supplier can provide a Vulnerability & Penetration testing report at an organization level which will include an executive summary and not the details of actual findings.

2. **Audits.** Supplier shall respond promptly to all reasonable security audit, scanning, discovery, and testing reports requested from Cisco, or from regulators (to the extent required by law) and shall cooperate and assist those regulators as required by law.

3. **Remedial Action.** If any audit or penetration testing exercise referred to above reveals any deficiencies, weaknesses or areas of non-compliance, Supplier shall promptly take such steps as may be required to remedy those deficiencies, weaknesses, and areas of non-compliance as soon as may be practicable in the circumstances and in any case within three (3) months of the findings from the audit and/or test.

4. **Status of Remedial Action.** Supplier shall keep Cisco informed of the status of any remedial action that is required to be carried out, including the estimated timetable for completing the same, and shall certify to Cisco as soon as may be practicable in the circumstances that all remedial actions have been completed.

xi. **Contractor Relationships**

1. **Policies**. Supplier shall have information security policies or procedures for its use of Contractors that impose requirements consistent with this SSE. Such policies shall be reviewed at planned intervals or if significant changes occur. Supplier shall have agreements with Contractors in which they agree to comply with Cisco's and/or Supplier's security requirements. Agreements with Contractors shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.

2. **Monitoring**. Supplier shall monitor and audit service delivery by its Contractors and review security against the agreements with Contractors. Supplier shall manage changes in Contractor services that may have an impact on security.

xii. **Management of Information Security Incidents and Improvements**

1. **Responsibilities and Procedures**. Supplier shall establish procedures to ensure a quick, effective, and orderly response to Information Security Incidents.

2. **Reporting Information Security Incident.** Supplier shall implement procedures for Information Security Incidents to be reported through appropriate management channels as quickly as possible. All employees and Contractors should be made aware of their responsibility to report Information Security Incidents as quickly as possible.

3. **Reporting Information Security Weaknesses.** Supplier, employees, and Contractors using information systems and services are required to note and report any observed or suspected information security weaknesses in systems or services.

4. **Assessment of and Decision on Information Security Events.** Supplier shall have an incident classification scale in place in order to decide whether a security event should be classified as an Information Security Incident. The classification scale is based on the impact and extent of an incident.

5. **Response Process.** Supplier shall maintain a record of Information Security Incidents with a description of the incident, the consequences of the incident, the name of the reporter and to whom the incident was reported, the procedure for rectifying the incident, and the remedial action taken to correct future security incidents.

xiii. **Information Security Aspects of Business Continuity Management**

1. **Planning**. Supplier shall maintain emergency and contingency plans for the facilities in which Supplier information systems that process Protected Data are located. To ensure that they are valid and effective during adverse situations, Supplier shall verify the established and implemented information security continuity controls at regular intervals.

2. **Data Recovery**. Supplier's redundant storage and its procedures for recovering data shall be designed to reconstruct Protected Data in its original state from before the time it was lost or destroyed.

5. **Notification and Communication Obligations**

a. **Notification**. Supplier shall immediately (i.e., within 24 hours) notify Cisco's Data Protection Incident Remedy team at:

data-incident-command@cisco.com

if any of the following events occur:

A any Information Security Incident or compromise of Protected Data;

B any security vulnerability, or weakness in Cisco's or customers' systems, or networks, or Supplier's systems or networks that could allow an attacker to compromise the integrity, availability, or confidentiality of the Protected Data;

C an Information Security Incident that compromises or could compromise the security of information and weaken or impair business operations;

D an Information Security Incident that negatively impacts the confidentiality, integrity, and availability of information that is processed, stored and transmitted using a computer in connection with Protected Data; or

E failure or inability to maintain compliance with the requirements of this SSE or Applicable Laws.

b. **Cooperation**

i. Supplier shall: (i) respond promptly to any Cisco communication(s); and (ii) provide all information, cooperation, and assistance to a Cisco designated response center.

c. **Information Security Communication**

i. Except as required by Applicable Laws, Supplier agrees that it will not inform any third party of any of the events described above in this Section without Cisco's prior written consent. Supplier shall fully cooperate with Cisco and any customer and with legal enforcement authorities concerning any actual or potential unauthorized access to Cisco's or customer's systems or networks, or Protected Data. Such co-operation shall include the retention of all information and data within Supplier's possession, custody, or control that is related to any Information Security Incident. If disclosure is required by law, Supplier will work with Cisco regarding the content of the disclosure to minimize any potential adverse impact upon Cisco and its customers. Supplier will bear the cost of reproduction or any other remedial steps necessary or advisable to address the suspected or actual incident or compromise.

d. **Post-Incident**

i. Supplier shall cooperate with Cisco in any post-incident investigation, remediation, and communication efforts. In addition, Supplier shall conduct a forensic and security review and audit in connection with any such Information Security Incident and, if appropriate to the nature and scope of the incident, retain an independent third party auditor to perform an audit or assessment of Supplier's information security procedures, systems, and network, including: testing of the system of controls; appropriate systems implementation and vulnerability analysis and penetration testing. In the event of the identification of any material security-related risk by Supplier, or the third party auditor, Supplier shall take timely remedial action based on industry best practices and the results of such assessment, audit or risk identification.

ATTACHMENT D

GLOSSARY OF TERMS

All capitalized terms not defined in this Glossary have the meanings set forth in the Agreement. In the event of a conflict between the definitions in the Agreement and any definitions in this Glossary, this Glossary will control as it relates to the subject matter set forth herein.

a. "**Agreement**" means all applicable agreements between the Cisco and the Supplier, including: Vendor Services Agreement, Master Service Agreement, Professional Services Subcontract Agreement, Supplier Base Agreement, and applicable licensing and other agreements under which the Supplier Performs.

b. **"Applicable Laws"** means any applicable country, federal, state, and local law, ordinances, statute, by-law, regulation, order, regulatory policy (including any requirement or notice of any regulatory body), compulsory guidance or industry code of practice, rule of court or directives, binding court decision or precedent, or delegated or subordinate legislation, each of the above as may be amended from time to time. Supplier will comply with all laws, all licenses, permits and approvals required by any government or authority, and shall comply with all applicable laws, rules, policies and procedures.

c. "**Approved Jurisdiction**" means a member state of the European Economic Area, or other jurisdiction as may be approved as having adequate legal protections for data by the European Commission currently found here: **http://ec.europa.eu/justice/data-protection/international transfers/adequacy/index_en.htm.**

d. "**Business Associate Agreement**" means the specific terms and conditions that apply when the Supplier Processes Protected Health Information.

e. "**Cardholder Data**" is a category of Sensitive Personal Data and includes a cardholder's name, full account number, expiration date, and the three-digit or four-digit security number printed on the front or back of a payment card.

f. "**Cisco Data**" means all information and data provided or made available to Supplier, including customer information and data, any manipulation of that data and any data or information Supplier collects, generates, or otherwise obtains in connection with its Performance under the Agreement. For clarity, to the extent Cisco Data contains Personal Data as defined herein, the terms related to Personal Data will also apply.

g. *"***EEA**" or "**European Economic Area**" means those countries that are members of European Free Trade Association ("**EFTA**"), and the then-current, post-accession member states of the European Union.

h. "**Electronic Protected Health Information**" or "**Electronic PHI**" shall have the meaning given to such term as set forth in the Business Associate Agreement.

i. "**EU Directives**" means the Data Protection Directive 95/46/EC and the Privacy and Electronic Communications Directive 2002/58/EC (and respective local implementing laws) concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), any amendments or replacements to them (such as the EU General Data Protection Regulation). For clarity, the EU Directives are a subset of Applicable Laws.

j. **"Generally Accepted Practices**" means those practices used by shall refer to the levels of accuracy, quality, care, prudence, completeness, timeliness, responsiveness, resource efficiency, productivity, and proactive monitoring of service performance that are at least equal to the then-

current accepted industry standards of first-tier providers of the tasks contemplated in Performance of the Agreement.

k. "**Information Security Incident"** means a suspected, successful, or imminent threat of unauthorized access, use, disclosure, breach, modification, theft, loss, corruption, or destruction of information; interference with information technology operations; or interference with system operations.

l. "**Performance**" means any acts by the Supplier in the course of completing obligations contemplated under the Agreement, including the performance of services, providing deliverables and work product, access to Personal Data, or providing Software as a Service ("SaaS"), cloud platforms or hosted services. "**Perform**," "**Performs**," and "**Performing**" shall be construed accordingly.

m. "**Process**" means any operation or set of operations that is performed upon Personal Data, whether or not by automatic means, such as collection, recording, securing, organization, storage, adaptation or alteration, access to, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction. "**Processes**" and "**Processing**" shall be construed accordingly.

n. "**Protected Data**" means Cisco Data, Confidential Information, Cisco customer Confidential Information and all Personal Data.

o. "**Protected Health Information**" or "**PHI**" shall have the meaning given to such term as set forth in the Business Associate Agreement and is a category of Personal Data. "Protected Health Information" includes "Electronic Protected Health Information" or "ePHI".

p. "**Representatives**" means Supplier and its affiliate's officers, directors, employees, agents, contractors, subcontractors and consultants.

q. "**Sensitive Personal Data**" or "**Special Categories of Data**" means personal information that requires an extra level of protection and a higher duty of care. These categories are defined by Applicable Law and include: information on medical or health conditions, certain financial information, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sexual preferences, precise geolocation over time, or information related to offenses or criminal convictions. Sensitive Personal Data and Special Categories of Data are each a category of Personal Data that are particularly sensitive and pose greater risk. Cisco may require additional privacy responsibilities when dealing with such Personal Data, which will be appended to the Agreement or a statement of work, as applicable.

r. "**Supplier**" means the person or legal entity, regardless of the form of organization that has entered into an Agreement with Cisco. Supplier may be defined as Subcontractor, Vendor, Contractor, Licensor, or other such defined term in the Agreement.