

**Carahsoft Rider to Manufacturer Commercial Supplier Agreements
(for U.S. Government End Users)
Revised 20161213**

- 1. Scope.** This Carahsoft Rider and the Manufacturer's Commercial Supplier Agreement (CSA) establish the terms and conditions enabling Carahsoft to provide Software and Services to U.S. Government agencies (the "Client" or "Licensee").

- 2. Applicability.** The terms and conditions in the attached Manufacturer's CSA are hereby incorporated by reference to the extent that they are consistent with Federal Law (e.g., the Anti-Deficiency Act (31 U.S.C. § 1341(a) (1) (B)), the Contracts Disputes Act of 1978 (41 U.S.C. § 601-613), the Prompt Payment Act, the Anti-Assignment statutes (31 U.S.C. § 3727 and 41 U.S.C. 15), 28 U.S.C. § 516 (Conduct of Litigation Reserved to Department of Justice (DOJ), and 28 U.S.C. § 1498 (Patent and copyright cases)). To the extent the terms and conditions in the Manufacturer's CSA is inconsistent with the Federal Law (*See* FAR 12.212(a)), they shall be deemed deleted and unenforceable under any resultant orders under Carahsoft's Multiple Award Schedule Contract, GS-35F-0119Y, including, but not limited to the following:
 - (a) Contracting Parties.** The Government customer (Licensee) is the "Ordering Activity", defined as an entity authorized to order under Government contracts as set forth in General Services Administration Order OGP 4800.2I, as may be revised from time to time. The Licensee cannot be an individual because any implication of individual licensing triggers the requirements for legal review by Federal Employee unions. Conversely, because of competition rules, the contractor must be defined as a single entity even if the contractor is part of a corporate group. The Government cannot contract with the group, or in the alternative with a set of contracting parties.

 - (b) Changes to Work and Delays.** Subject to General Services Administration Acquisition Regulation (GSAR) 552.238-81 Modifications (Federal Supply Schedule) (APR 2014) (Alternate I – APR 2014) and GSAR 552.212 -4 (f) Contract Terms and Conditions – Commercial Items, Excusable Delays (MAY 2015) (Alternate II – JUL 2009) (FAR Deviation – JUL 2015) (Tailored) regarding which of the GSAR and the FAR provisions shall take precedence.

 - (c) Contract Formation.** Subject to FAR Sections 1.601(a) and 43.102, the Government Order must be signed by a duly warranted contracting officer, in writing. The same requirement applies to contract modifications affecting the rights of the parties. All terms and conditions intended to bind the Government must be included within the contract signed by the Government.

- (d) Audit.** During the term of this CSA: (a) If Ordering Activity's security requirements included in the Order are met, Manufacturer or its designated agent may audit Ordering Activity's facilities and records to verify Ordering Activity's compliance with this CSA. Any such audit will take place only during Ordering Activity's normal business hours contingent upon prior written notice and adherence to any security measures the Ordering Activity deems appropriate, including any requirements for personnel to be cleared prior to accessing sensitive facilities. Carahsoft on behalf of the Manufacturer will give Ordering Activity written notice of any non-compliance, including the number of underreported Units of Software or Services ("Notice"); or (b) If Ordering Activity's security requirements are not met and upon Manufacturer's request, Ordering Activity will run a self-assessment with tools provided by and at the direction of Manufacturer ("Self-Assessment") to verify Ordering Activity's compliance with this CSA.
- (e) Termination.** Clauses in the Manufacturer's CSA referencing suspension, termination or cancellation of the Manufacturer's CSA, the License, or the Customer's Account are hereby deemed to be deleted. Termination, suspension or cancellation shall be governed by the GSAR 552.212-4 and the Contract Disputes Act, 41 U.S.C. §§ 601-613, subject to the following exceptions:
- Carahsoft may request cancellation or termination of the CSA on behalf of the Manufacturer if such remedy is granted to it after conclusion of the Contracts Disputes Act dispute resolutions process referenced in Section (q) below or if such remedy is otherwise ordered by a United States Federal Court.
- (f) Consent to Government Law / Consent to Jurisdiction.** Subject to the Contracts Disputes Act of 1978 (41 U.S.C §§ 7101-7109) and Federal Tort Claims Act (28 U.S.C. §1346(b)). The validity, interpretation and enforcement of this Rider and the CSA will be governed by and construed in accordance with the laws of the United States. All clauses in the Manufacturer's CSA referencing equitable remedies are deemed not applicable to the Government order and are therefore deemed to be deleted.
- (g) Force Majeure.** Subject to GSAR 552.212 -4 (f) Contract Terms and Conditions – Commercial Items, Excusable Delays (MAY 2015) (Alternate II – JUL 2009) (FAR Deviation – JUL 2015) (Tailored). Unilateral Termination by the Contractor does not apply to a Government order and all clauses in the Manufacturer's CSA referencing unilateral termination rights of the Manufacturer's CSA are hereby deemed to be deleted.
- (h) Assignment.** All clauses regarding Assignment are subject to FAR Clause 52.232-23, Assignment of Claims (MAY 2014) and FAR 42.12 Novation and Change-of-Name Agreements, and all clauses governing Assignment in the Manufacturer's CSA are hereby deemed to be deleted.
- (i) Waiver of Jury Trial.** All clauses referencing waiver of Jury Trial are subject to FAR Clause 52.233-1, Disputes (MAY 2014), and all clauses governing waiver of jury trial in the Manufacturer's CSA are hereby deemed to be deleted.

- (j) Customer Indemnities.** All of the Manufacturer's CSA clauses referencing Customer Indemnities are hereby deemed to be deleted.
- (k) Contractor Indemnities.** All of the Manufacturer's CSA clauses that (1) violate DOJ's right (28 U.S.C. 516) to represent the Government in any case and/or (2) require that the Government give sole control over the litigation and/or settlement, are hereby deemed to be deleted.
- (l) Renewals.** All of the Manufacturer's CSA clauses that violate the Anti-Deficiency Act (31 U.S.C. 1341, 41 U.S.C. 11) ban on automatic renewal are hereby deemed to be deleted.
- (m) Future Fees or Penalties.** All of the Manufacturer's CSA clauses that violate the Anti-Deficiency Act (31 U.S.C. 1341, 41 U.S.C. 11), which prohibits the Government from paying any fees or penalties beyond the Contract amount, unless specifically authorized by existing statutes, such as the Prompt Payment Act, or Equal Access To Justice Act 31 U.S.C. 3901, 5 U.S.C. 504 are hereby deemed to be deleted.
- (n) Taxes.** Taxes are subject to GSAR 552.212-4(k) Contract Terms and Conditions – Commercial Items, Taxes (MAY 2015) (Alternate II – JUL 2009) (FAR Deviation – JUL 2015) (Tailored) and GSAR 552.212-4 (w) (1) (x) Contract Terms and Conditions – Commercial Items, Taxes (MAY 2015) (Alternate II – JUL 2009) (FAR Deviation – JUL 2015) (Tailored).
- (o) Third Party Terms.** Subject to the actual language agreed to in the Order by the Contracting Officer. Any third party manufacturer will be brought into the negotiation, or the components acquired separately under Federally-compatible agreements, if any. Contractor indemnities do not constitute effective migration.
- (p) Installation and Use of the Software.** Installation and use of the software shall be in accordance with the Rider and Manufacturer's CSA, unless an Ordering Activity determines that it requires different terms of use and Manufacturer agrees in writing to such terms in a valid task order placed pursuant to the Government contract.
- (q) Dispute Resolution and Venue.** Any disputes relating to the Manufacturer's CSA and to this Rider shall be resolved in accordance with the FAR, the GSAR and the Contract Disputes Act, 41 U.S.C. §§ 7101-7109. See GSAR 552.212-4 (w) (1) (iii) Contract Terms and Conditions – Commercial Items, Law and Disputes (MAY 2015) (Alternate II – JUL 2009) (FAR Deviation – JUL 2015) (Tailored). The Ordering Activity expressly acknowledges that Carahsoft, as the vendor selling the Manufacturer's licensed software, shall have standing under the Contract Disputes Act to bring such claims that arise out of licensing terms incorporated into Multiple Award Schedule Contract GS-35F-0119Y.

(r) Limitation of Liability: Subject to the following:

Carahsoft, Manufacturer and Ordering Activity shall not be liable for any indirect, incidental, special, or consequential damages, or any loss of profits, revenue, data, or data use. Further, Carahsoft, Manufacturer and Ordering Activity shall not be liable for punitive damages except to the extent this limitation is prohibited by applicable law. This clause shall not impair the U.S. Government's right to recover for fraud or crimes arising out of or related to this Government Contract under any federal fraud statute, including the False Claims Act, 31 U.S.C. §§ 3729-3733.

(s) Advertisements and Endorsements. Unless specifically authorized by an Ordering Activity in writing, such use of the name or logo of any U.S. Government entity is prohibited.

(t) Public Access to Information. Manufacturer agrees that the CSA and this Rider contain no confidential or proprietary information and acknowledges the CSA and this Rider will be available to the public.

(u) Confidentiality. Any provisions that require the Licensee to keep certain information confidential are subject to the Freedom of Information Act, 5 U.S.C. §552, and any order by a United States Federal Court. The Licensee may provide information to other components of the United States Government pursuant to proper requests for such information as permitted by law, regulation or policy (e.g., disclosures to Congress, auditors, Inspectors General, etc.).

**CIS CYBERSECURITY SERVICES
END USER TERM AND CONDITIONS**

These terms and conditions shall apply to the purchase of any Cyber Security Services (as defined below) purchased by you (the “**End User**”) from Center for Internet Security, Inc. (“**CIS**”) under Carahsoft Technology Corporation’s (Carahsoft’s) GSA Schedule 70 Contract (the “**Contract**”). By accepting purchase of Cyber Security Services under the Contract, you agree to be bound by these terms and conditions.

I. Definitions

A. **Security Operation Center (SOC)** – 24 X 7 X 365 watch and warning center that provides network monitoring, dissemination of cyber threat warnings and vulnerability identification and mitigation recommendations.

B. **Cyber Security Services.** Cyber Security Services consist of the following services, plus any additional services as CIS may add in the future:

1. Network Security Monitoring and Analysis Service: Intrusion detection system (IDS) monitoring and analysis of related data; event notification and delivery; and management of associated devices, including software necessary for service delivery. Also referred to as Albert monitoring services.

2. Cyber Security Consulting Service: customized cyber security services, including without limitation, external network penetration testing, social engineering (e.g. phishing assessments) and comprehensive security reviews.

II. Terms for Device Monitoring Services

The following terms and conditions apply to the purchase of Device Monitoring Services:

A. CIS Responsibilities

1. CIS will provide the following:

a. 24/7 telephone (1-866-787-4722) availability for assistance with events detected by the CSS.

b. Analysis of logs from monitored security devices for attacks and malicious traffic.

c. Analysis of security events.

d. Correlation of security data/logs/events with information from other sources.

e. Notification of security events per the Escalation Procedures provided by End User.

2. CIS will process batch queries of Netflow data upon End User request, with a limit of 10 queries per month. CIS maintains flow records for a period of five (5) months.

B. End User Responsibilities

1. End User acknowledges and agrees that CIS's ability to perform the Device Monitoring Services purchased or provided by CIS for the benefit of End User is subject to End User fulfilling certain responsibilities listed below. End User acknowledges and agrees that CIS does not have any responsibility whatsoever to perform or to continue to perform Device Monitoring Services in the event End User fails to meet its responsibilities described below.
2. End User acknowledges and agrees that only those security devices supported by CIS fall within the scope of this Agreement. End User will ensure the correct functioning of devices except where End User selects Managed Security Services in which CIS manages the device(s).
3. End User shall provide logistic support in the form of rack space, electricity, Internet connectivity, and any other infrastructure necessary to support communications at End User's expense.
4. End User shall provide the following to CIS prior to the commencement of Device Monitoring Services and at any time during the Term of the Contract if the information changes:
 - a. Current network diagrams to facilitate analysis of security events on the portion(s) of End User's network being monitored. Network diagrams will need to be revised whenever there is a substantial network change;
 - b. Reasonable assistance to CIS, including, but not limited to, providing all technical and license information related to the Service(s) reasonably requested by CIS, to enable CIS to perform the Service(s) for the benefit of End User;
 - c. Supply onsite hardware, virtual machines or software that is necessary in providing Device Monitoring Services. End User also agrees onsite hardware, virtual machines and software will meet specifications set forth by CIS;
 - d. Maintenance of all required hardware, virtual machines, or software necessary for the log collection platform located at End User's site, and enabling access to such hardware, virtual machines, or software as necessary for CIS to provide services;
 - e. Public and Private IP address ranges including a list of servers being monitored including the type, operating system and configuration information;
 - f. Completed Pre-Installation Questionnaires (PIQ). The PIQ will need to be revised whenever there is a change that would affect CIS's ability to provide the Device Monitoring Services;
 - g. A completed Escalation Procedure Form including the name, e-mail address and 24/7 contact information for all designated Points of Contact (POC); and
 - h. The name, email address, and landline, mobile, and pager numbers for all shipping, installation and security points of contact.

5. End User shall provide the following with respect to any Device Monitoring Services during the Term:

- a. Written notification to CIS SOC (SOC@cisecurity.org) at least thirty (30) days in advance of changes in hardware or network configuration affecting CIS's ability to provide Cyber Device Monitoring Services;
- b. Written notification to CIS SOC (SOC@cisecurity.org) at least twelve (12) hours in advance of any scheduled downtime or other network and system administration scheduled tasks that would affect CIS's ability to provide the service;
- c. A revised Escalation Procedure Form must be submitted when there is a change in status for any POC.
- d. Sole responsibility for maintaining current maintenance and technical support contracts with End User's software and hardware vendors for any device subject to Device Monitoring Services that has not been supplied by CIS;
- e. Active involvement with CIS SOC to resolve any tickets requiring End User input or action; and
- f. Reasonable assistance in remotely installing and troubleshooting devices including hardware and communications.

III. Additional Terms for Cyber Security Consulting Services

Because of the individualized nature of the Cyber Security Consulting Services, all such services will be scoped by a separate Statement of Work, to be agreed upon by the parties. Such Statements of Work will be subject to the applicable terms and conditions set forth herein.

IV. Title, Limitation of Warranties and Liability

A. Title. CIS will at all times retain title to hardware and/or software provided to End User during the Term of this Agreement. Upon termination or expiration (including non-renewal) of this Agreement, End User will return all hardware and/or software provided under this Agreement within thirty (30) days of such expiration or termination.

The End User shall own all right, title and interest in its data that is provided to CIS pursuant to this Agreement. End User hereby grants CIS a non-exclusive, non-transferable license to access and use such data to the extent necessary to provide Cyber Security Services under this Agreement.

B. LIMITATION OF LIABILITY. CIS DOES NOT ASSUME ANY RESPONSIBILITY OR LIABILITY FOR ANY ACT OR OMISSION OR OTHER PERFORMANCE RELATED TO THE PROVISION OF CYBER SECURITY SERVICES, INCLUDING ANY ACT OR OMISSION BY CONTRACTORS OR SUBCONTRACTORS OF CIS, OR FOR THE ACCURACY OF THE INFORMATION PROVIDED AS PART OF THE SERVICES. THE SERVICES ARE PROVIDED ON AN "AS-IS" BASIS, WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED.

V. Confidentiality Obligation

CIS acknowledges that certain confidential or proprietary information may either be provided by End User to CIS or generated in the performance of the Cyber Security Services, including without limitation: information regarding the infrastructure and security of End User information systems; assessments and plans that relate specifically and uniquely to the vulnerability of End User information systems; the results of tests of the security of End User information systems insofar as those results may reveal specific vulnerabilities; or information otherwise marked as confidential by End User (“Confidential Information”). The End User acknowledges that it may receive from CIS trade secrets and confidential and proprietary information (“Confidential Information”). Both Parties agree to hold each other’s Confidential Information in confidence to the same extent and the same manner as each party protects its own confidential information, but in no event will less than reasonable care be provided and a party’s information will not be released in any identifiable form without the express written permission of such party or as required pursuant to lawfully authorized subpoena or similar compulsive directive or is required to be disclosed by law, provided that the End User shall be required to make reasonable efforts, consistent with applicable law, to limit the scope and nature of such required disclosure. CIS shall, however, be permitted to disclose relevant aspects of such Confidential Information to its officers, directors and employees, provided that they agree to protect the Confidential Information to the same extent as required under this Agreement. The Parties agree to use all reasonable steps to ensure that Confidential Information received under this Agreement is not disclosed in violation of this Section V. The obligations of the Parties pursuant to this paragraph shall survive the termination of this Agreement. Nothing in this Agreement shall prohibit CIS from using aggregated data of its End Users in any format for any purpose, provided that such data cannot be identified to or associated with End User.

VI. Force Majeure

Neither Party shall be liable for performance delays or for non-performance due to causes beyond its reasonable control.

VII. No Third Party Rights

Nothing in this Agreement shall create or give to third parties any claim or right of action of any nature against End User or CIS.

VIII. Assignment

Neither Party may assign their rights and obligations under this Agreement without the prior written approval of the other party, which approval shall not be unreasonably withheld, conditioned or delayed. This Agreement shall be binding upon and inure to the benefits of each Party and their respective successors and assigns.

IX. Notices

- A. All notices permitted or required hereunder shall be in writing and shall be transmitted either: via certified or registered United States mail, return receipt requested; by facsimile transmission; by personal delivery; by expedited delivery service; or by e-mail with acknowledgement of receipt of the notice. End User shall provide CIS with the appropriate contact information.

Such notices shall be addressed as follows or to such different addresses as the Parties may from time-to-time designate:

CIS

Name: Mark Perry
Title: Program Executive
Address: Center for Internet Security, Inc.
31 Tech Valley Drive
East Greenbush, NY 12061-4134
Phone: (518) 266-3476
E-Mail: mark.perry@cisecurity.org

B. Any such notice shall be deemed to have been given either at the time of personal delivery or, in the case of expedited delivery service or certified or registered United States mail, as of the date of first attempted delivery at the address and in the manner provided herein, or in the case of facsimile transmission or email, upon receipt.

C. The Parties may, from time to time, specify any new or different contact information as their address for purpose of receiving notice under this Agreement by giving fifteen (15) days written notice to the other Party sent in accordance herewith. The Parties agree to mutually designate individuals as their respective representatives for the purposes of receiving notices under this Agreement. Additional individuals may be designated in writing by the Parties for purposes of implementation and administration, resolving issues and problems and/or for dispute resolution.

X. Governing Law and Jurisdiction

Any disputes arising in connection with this Agreement shall be governed and interpreted by the federal laws of the United States.

XI. Non-Waiver

None of the provisions of this Agreement shall be considered waived by either Party unless such waiver is given in writing by the other party. No such waiver shall be a waiver or any past or future default, breach or modification of any of the terms, provision, conditions or covenants of the Agreement unless expressly set forth in such waiver.

XII. Entire Agreement; Amendments

This Agreement, the terms and conditions of Carahsoft's GSA Multiple Award 70 Contract, and the appendices attached hereto constitute the entire understanding and agreement between the Parties with respect to the subject matter hereof and replace and supersede all prior understandings, communications, agreements or arrangements between the parties with respect to this subject matter, whether oral or written. This Agreement may only be amended as agreed to in writing by the GSA Contracting Officer and Carahsoft.

XIII. Partial Invalidity

If any provision of this Agreement be adjudged by a court of competent jurisdiction to be unenforceable or invalid, that provision shall be limited or eliminated to the minimum extent necessary so that this Agreement shall otherwise remain in full force and effect and enforceable.

CENTER FOR INTERNET SECURITY, INC.
CIS SECURESUITE END USER MEMBERSHIP TERMS

I. Definitions

Affiliate means any corporation, firm, limited liability company, partnership or other entity that directly or indirectly controls or is controlled by or is under common control with a Party.

CIS Benchmarks means consensus based secure configuration guidelines applicable to a variety of operating systems, middleware and software applications, and network devices, designed to assess Customer's network cybersecurity.

CIS Controls means the CIS Critical Security Controls for Effective Cyber Defense, v. 6.1 and later.

CIS SecureSuite means the cybersecurity configuration and remediation membership offerings provided by CIS, as set forth in these Terms.

CIS SecureSuite Products includes any or all of the following: CIS Benchmarks and CIS Controls in any format provided, CIS-CAT Pro (including CIS-CAT Pro Assessor and CIS-CAT Pro Dashboard as described below), CIS Workbench community site, product guides, remediation content and other products offered by CIS from time to time.

II. Membership Benefits. Subject to the terms and conditions set forth herein (the "Terms"), CIS grants to Customer a one (1) year CIS SecureSuite End User Organization membership that entitles Customer to the following benefits:

A. Organizational Use

1. Access to and use of the CIS configuration assessment tool ("**CIS-CAT Pro**"), including use of the following:
 - a. CIS CAT Pro Assessor, allowing Customer to analyze and score the configuration of Customer's internal information technology systems and obtain a score between 1-100 for conformity against CIS Benchmarks including CIS Benchmark recommendations to one of more of the CIS Controls and subcontrols; and
 - b. CIS-CAT Pro Dashboard, allowing Customer to: analyze multiple CIS Benchmarks in a single view for comparison, multiple device reviews; access a CIS Controls view for any annotated CIS Benchmark content; view individual CIS-CAT Pro assessment results, including the ability to create exceptions and recalculate the CIS-CAT Pro assessment; and create individual reporting in multiple formats.
2. The right to use and distribute the CIS SecureSuite Products within and throughout Customer's organization;
3. Unlimited access to and use of the CIS Workbench (a community site where CIS SecureSuite resources are developed) for access to CIS SecureSuite Products, including forums for information sharing, user support, and discussions among members, developers, and CIS staff;
4. Timely electronic notification of updates to the CIS Benchmarks, CIS Controls and CIS-CAT Pro;
5. Enhanced CIS Benchmark and CIS-CAT Pro support from CIS staff and developers;
6. The right to use the CIS SecureSuite membership mark (as set forth on Exhibit A) on Customer's websites and documents; and
7. Access to any additional CIS SecureSuite products or other membership benefits offered by CIS from time to time.

B. *End User Membership Restrictions*

1. The Customer agrees that the Customer may not sell or resell any SecureSuite Product, or distribute any CIS SecureSuite Product outside of Customer's organization.
2. The Customer agrees that the Customer use of CIS SecureSuite Products is limited to internal use to secure organization's owned system/network(s) and data, and not that of any third party.

III. CIS SecureSuite Products Provided As Is. CIS makes reasonable efforts to utilize and maintain the most current network security and antivirus protection programs available to screen and protect CIS's computer programs, websites, and computer infrastructure from malware. However, Customer understands and agrees that CIS is providing the CIS SecureSuite Products "as is" and "as available" without any representations, warranties, or covenants of any kind whatsoever, including: (i) the effect or lack of effect of any CIS SecureSuite Product on the operation or the security of any network, system, software, hardware, or any component of any of them; and (ii) the accuracy, utility, reliability, timeliness, or completeness of any CIS SecureSuite Product.

IV. Ownership Rights of Intellectual Property and Products Reserved. Customer is not acquiring any title or ownership rights in or to any of the CIS SecureSuite Products or associated intellectual property, and full title and all ownership rights to the CIS SecureSuite Products and associated intellectual property remain the exclusive property of CIS. All rights to the CIS SecureSuite Products not expressly granted in these Terms are hereby reserved.

V. Restrictions. Customer acknowledges and agrees that Customer may not: (A) decompile, disassemble, alter, reverse engineer, or otherwise attempt to derive the source code for any CIS SecureSuite Product (except to the extent that such product is already in the form of source code); (B) distribute or redistribute (except as permitted in Section I(A)(2), sell, rent, lease, sublicense or otherwise transfer or exploit any rights to any CIS SecureSuite Product in any way or for any purpose; (C) post any CIS SecureSuite Product on any website, bulletin board, ftp server, newsgroup, or other similar mechanism or device; (D) remove from or alter the terms of use placed on any CIS SecureSuite Product; (E) remove or alter any proprietary notices on any CIS SecureSuite Product; (F) except to the extent permitted under Section II, Membership Benefits, create any derivative work based directly on an CIS SecureSuite Product or any component thereof; (G) represent or claim a particular level of compliance or consistency with any CIS SecureSuite Product; or (I) facilitate or otherwise aid other individuals or entities in violating these Terms.

VI. Customer's Responsibility to Evaluate Risks. Customer acknowledges and agrees that: (A) no network, system, device, hardware, software, or component can be made fully secure; (B) Customer has the sole responsibility to evaluate the risks and benefits of the CIS SecureSuite Products to Customer's particular circumstances and requirements; and (C) except as otherwise provided herein, CIS does not assume any of the liabilities associated with Customer's use of any or all of the CIS SecureSuite Products.

VII. CIS Indemnification of Customer. CIS shall indemnify, defend, and hold Customer harmless against any claim, suit or proceeding (including reasonable attorneys' fees) brought against Customer alleging that the CIS SecureSuite Products infringe any patent, copyright, or enforceable trade secret, provided that Customer: (A) gives CIS prompt written notice of any such claim; (B) allows CIS to control the defense and settlement of such claim; (C) refrains from entering into any settlement or compromise of such claim without CIS's prior written consent; and (D) provides all assistance reasonably requested by CIS in the defense or settlement of such claim, at CIS's expense, provided further that, at Customer's option, CIS shall grant Customer an immediate right to terminate its membership, in which case, Customer's sole and exclusive remedy shall be to terminate its membership, to cease using and to return to CIS all copies of the CIS SecureSuite Products in Customer's possession and receive a pro rata portion return of any fees paid. THIS SECTION SETS FORTH CIS'S SOLE AND EXCLUSIVE LIABILITY, AND CUSTOMER'S SOLE AND EXCLUSIVE REMEDY FOR CIS'S INFRINGEMENT OF THIRD PARTY RIGHTS OF ANY KIND.

VIII. Confidential Information.

- A. *Confidential Information.* Each party acknowledges that by reason of its relationship with the other party hereunder, such party (the “**Receiving Party**”) might receive access to certain information and materials concerning the other party’s (the “**Disclosing Party**”). “Confidential Information” means oral or written non- public information that the Disclosing Party designates as being confidential or which, under the circumstances surrounding disclosure, ought to be treated as confidential, whether provided to the Receiving Party before, on or after the date hereof. “Confidential Information” includes, without limitation, information relating to the Disclosing Party’s software and hardware products, specifications, databases, networks, systems design, file layouts, tool combinations and development methods, and information relating to the Disclosing Party’s business or financial affairs, such as business methods, marketing strategies, pricing, product development strategies and methods, customer lists and financial results. “Confidential Information” also includes information received from others that the Disclosing Party is obligated to treat as confidential. “Confidential Information” includes all tangible materials which contain Confidential Information, including, without limitation, written or printed documents, computer disks or tapes, and other magnetic or optical storage media, whether user- or machine-readable.
- B. *Exclusions.* Confidential Information does not include any information that the Receiving Party can demonstrate: (i) was known to the Receiving Party prior to its disclosure hereunder by the Disclosing Party; (ii) was independently developed by the Receiving Party; (iii) is or becomes publicly known through no wrongful act of the Receiving Party; (iv) has been rightfully received from a third party whom the Receiving Party has reasonable grounds to believe is authorized to make such disclosure without restriction; or (v) has been approved for public release by the Disclosing Party’s prior written authorization. Confidential Information may be disclosed pursuant to applicable law, regulations or court order, provided that the Receiving Party provides, where reasonably possible, prompt advance notice thereof to enable the Disclosing Party to seek a protective order or otherwise prevent such disclosure.
- C. *Use.* The Receiving Party acknowledges and agrees that the Disclosing Party’s Confidential Information is of substantial value to the Disclosing Party, which value would be harmed if such information were disclosed to third parties. The parties agree that, commencing on the Effective Date and thereafter, they will not: (i) use the Disclosing Party’s Confidential Information in any way, except in the performance of obligations under these Terms; or (ii) disclose the Disclosing Party’s Confidential Information to any third party, except to the Receiving Party’s employees who need to know such information, provided such employees have a signed confidentiality agreement with terms no less restrictive than those contained these Terms. The parties will not publish, in any form, the other party’s Confidential Information beyond any descriptions published by said other party.
- D. *Ownership of Information.* The parties expressly agree that the Disclosing Party shall retain all ownership in its Confidential Information.
- E. *Return of Information.* In the event of any termination or expiration of this or any other agreement between the parties: (i) upon the written request of the Disclosing Party, the Receiving Party shall return all copies of Confidential Information to the Disclosing Party; and (ii) except to the extent the Receiving Party is advised in writing by counsel that there is a legal prohibition on so doing, the Receiving Party will also promptly destroy all written material, memoranda, notes and other writings or recordings whatsoever prepared by it or its representatives based upon, containing or otherwise reflecting any Confidential Information of the Disclosing Party. Any Confidential Information that is not returned or destroyed including, without limitation, any oral Confidential Information, shall remain subject to the confidentiality obligations set forth in these Terms. The Receiving Party may return the Confidential Information, or any part thereof, to the Disclosing Party at any time.
- F. *Duration.* All obligations to protect Confidential Information set forth in these Terms shall apply during the time of the relationship between the parties and thereafter, without limitation.

IX. Additional Terms

- A. *Jurisdiction.* Customer acknowledges and agrees that these Terms and Customer's membership will be governed by and construed in accordance with the federal laws of the United States.

- B. *Notices.* All notices, requests, demands and determinations made under these Terms (other than routine operational communications) shall be in writing and shall be deemed duly given (A) when delivered personally (against a signed receipt), (B) on the designated day of delivery (other than a weekend or Federal holiday) after being timely given to an express overnight courier with a reliable system for tracking delivery, or (C) six (6) days after the day of mailing, when sent by first class United States mail, postage prepaid and return receipt requested, to the address set forth below and to the attention of the undersigned.

EXHIBIT A

CIS SECURESUITE MEMBERSHIP MARK



CIS SecureSuite
Membership