Carahsoft Supplier Code of Conduct

Background: Carahsoft operates with high standards and expectations and expects our resellers partners, subcontractors, suppliers, and other supply chain members to do the same.

To maintain excellence throughout all aspects of business, we continue to enhance the way we engage with our Suppliers to encourage continual improvement of the way we, and our supplier base, address and manage important issues. Our revised expectations and minimum standards within the enclosed document are the product of not only the increasing regulatory environment globally with respect to particular issues, but also the increasing expectations of our clients and the wider community.

Carahsoft values our Supplier relationships and is committed to working with, and supporting, our Suppliers to achieve mutual objectives. A Supplier's performance and adherence to high business standards is an important and integral part of the value chain for Carahsoft. Carahsoft promotes and expects the application of high legal, ethical, environmental and employee-related standards within our own business and among our Suppliers.

This Supplier Code of Conduct sets forth the minimum standards of business conduct that we expect from all of our suppliers:

ETHICS

The highest standard of integrity is expected in all of our business dealings. Any and all forms of corruption, extortion, bribery (including facilitation payments), and embezzlement are strictly prohibited and may result in immediate termination and legal action:

- Suppliers will not offer or provide money or anything of value to any person if the circumstances indicate that it is probable that all or part of the money or other thing of value is being given to another individual or entity to influence official action or to obtain a business advantage.
- Suppliers are expected to understand relevant Carahsoft and government gift and hospitality policies before offering or providing Carahsoft and government personnel with any gift and/or business entertainment. Gifts or entertainment should never be offered to Carahsoft and government personnel or representatives under circumstances that create the appearance of impropriety.
- Suppliers must comply with all applicable trade control laws and regulations in the import, export, re-export or transfer of goods and services (including software and technology). All invoices and any customs or similar documentation submitted to Carahsoft or governmental authorities in connection with transactions involving Carahsoft must accurately describe the goods and services provided and the price thereof.
- Suppliers shall not share or exchange any prices, costs, or other competitive information, or undertaking of any collusive conduct with any other third party to Carahsoft with respect to any proposed, pending or current Carahsoft procurement.
- Suppliers will use only subcontractors or other third parties who comply with all applicable laws and regulations, and who adhere to the same (minimum) standards set forth in this guide when contracting or doing business with Carahsoft.

WHISTLEBLOWER PROTECTION

Suppliers should ensure that their employees have all the rights and protections against reprisals as provided by law and regulation. These rights and protections include, for example, those in 41 U.S.C. 4712 (implemented by FAR 52.203-17, Contractor Employee Whistleblower Rights and Requirement to Inform Employees of Whistleblower Rights), 10 U.S.C. 2409 (implemented in DFARS 203.9, Whistleblower Protections for Contractor Employees), and 18 U.S.C. 1833(b) (Immunity from Liability for Confidential Disclosure of a Trade Secret to the Government or in a Court Filing).

CONTERFEIT RISK

All material, including material incorporated into the Goods delivered under a Purchase Order must be procured from the original equipment or component manufacturer (OEM/OCM), or the OEM/OCM's authorized distributor. Independent distributors or brokers are not acceptable and shall not be used by Suppliers to provide product delivered under a Purchase Order. Suppliers shall maintain a counterfeit risk mitigation process in accordance with industry recognized standards.

CONTERFEIT ELECTRONIC PARTS

As applicable, Supplier certifies that it has an established Counterfeit Electronic Part Detection and Avoidance System satisfying all requirements under Defense Federal Acquisition Regulation Supplement ("DFARS") clause 252.246-7007.

NO REFURBISHED PARTS

Supplier certifies that all products provided to Carahsoft or its customers as new, composed of previously unused components, whether manufactured from virgin material, covered material in the form of raw material, or materials and by-products generated from, and reused within, an original manufacturing process. All used, refurbished, or reconditioned products shall not be accepted and shall be returned and refunded at Supplier's expense. Supplier shall be liable for any expenses incurred for the supply of such prohibited items.

IMPORT; EXPORT SALES

Supplier agrees that it will not export, re-export, directly or indirectly, any United States origin commodities, technology/technical data or software sold to Carahsoft or its customers, or any direct product of that technical data: (i) in violation of the export laws and regulations of the United States, including but not limited to, the Bureau of Industry and Security Export Administration Regulations and the regulations of the Treasury Department's Office of Foreign Assets Control or any other relevant national government authority; (ii) to any country for which an export license or other governmental approval is required at the time of export, without first obtaining all necessary export licenses or other approvals; (iii) to any country or national or resident of a country to which trade is embargoed by the United States; (iv) to any person or firm on any government agencies Restricted Party List, including, but not limited to the U.S. Department of Commerce's Table of Denial Orders or Entities list, or U.S Treasury Department's list of Specially Designated Nationals; or (v) for use in any sensitive nuclear, chemical or biological weapons, or missile technology end-uses unless authorized by the U.S. Government by regulation or specific license.

SAM.GOV REGISTRATION

Supplier represents and warrants that it has an active SAM.GOV Registration in accordance with 52.204-7, System for Award Management (Oct 2018).

DEBARMENT OR SUSPENSION

By accepting any Purchase Order from Carahsoft, Supplier represents and warrants that as of the Purchase Order effective date, Supplier or its principals are not currently debarred, suspended, or proposed for debarment or suspension by the Federal Government or any state agency.

COMPLIANCE WITH LAWS

Suppliers shall comply with all applicable federal, state, and local laws and ordinances and all pertinent lawful orders, rules, and regulations and such compliance shall be a material requirement of this Agreement, as applicable. Flowdown provisions are also to be adhered to

- 3.502-2, Subcontractor kickbacks (Sep 2023).
- 52.203-5, Covenant Against Contingent Fees (May 2014).
- 52.203-7, Anti-Kickback Procedures (Jun 2020).
- 52.203-13, Contractor Code of Business Ethics and Conduct (Jun 2020) (41 U.S.C. 3509).
- 52.203-19, Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements (Jan 2017) (section 743 of Division E, Title VII, of the Consolidated and Further Continuing Appropriations Act, 2015 (Pub. L. 113-235) and its successor provisions in subsequent appropriations acts (and as extended in continuing resolutions).
- 52.204-23, Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities (Nov 2021) (Section 1634 of Pub. L. 115-91).
- 52.204-24, Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment (Aug 2020).
- 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment. (Nov 2021) (Section 889(a)(1)(A) of Pub. L. 115-232).
- 52.204-26, Covered Telecommunications Equipment or Services-Representation (Oct 2020).
- 52.204-27, Prohibition on ByteDance Covered Application (Jun 2023).
- 52.211-5, Material Requirements (Aug 2000).
- 52.219-8, Utilization of Small Business Concerns (Oct 2022) (15 U.S.C. 637(d)(2) and (3)), in all subcontracts that offer further subcontracting opportunities. If the subcontract (except subcontracts to small business concerns) exceeds the applicable threshold specified in the FAR 19.702 (a) on the date of the subcontract award, the subcontractor must include 52.219-8 in lower tier subcontracts that offer subcontracting opportunities.
- 52.222-21, Prohibition of Segregated Facilities (Apr 2015).
- 52.222-26, Equal Opportunity (Sep 2016) (E.O. 11246).
- 52.222-35, Equal Opportunity for Veterans (Jun 2020) (38 U.S.C. 4212).
- 52.222-36, Equal Opportunity for Workers with Disabilities (Jun 2020) (29 U.S.C. 793).
- 52.222-37, Employment Reports on Veterans (Jun 2020) (38 U.S.C. 4212).
- 52.222-40, Notification of Employee Rights under the National Labor Relations Act (Dec 2010) (E.O. 13496). Flow down required in accordance with paragraph (f) of FAR clause 52.222-40.

- 52.222-41, Service Contract Labor Standards (Aug 2018) (41 U.S.C. chapter 67).
- 52.222-50, (1) Combating Trafficking in Persons (Nov 2021) (22 U.S.C. chapter 78 and E.O. 13627).
- 52.222-51, Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment – Requirements (May 2014) (41 U.S.C. chapter 67)
- 52.222-53, Exemption from Application of the Service Contract Labor Standards to Contracts for Certain Services – Requirements (May 2014) (41 U.S.C. chapter 67).
- 52.222.54, Employment Eligibility Verification (May 2022) (E.O. 12989).
- 52.222-55, Minimum Wages Under Executive Order 13658 (Jan 2022).
- 52.222-62, Paid Sick Leave Under Executive Order 13706 (Jan 2022) (e.o. 13706).
- 52.223-15, Energy Efficiency in Energy Consuming Products (May 2020).
- 52.224-1, Privacy Act Notification (Apr 1984).
- 52.224-2, Privacy Act (Apr 1984).
- 52.224-3, Privacy Training (Jan 2017) (5 U.S.C. 552a).
- 52.225-13, Restrictions on Certain Foreign Purchases (Feb 2021).
- 52.225-26, Contractors Performing Private Security Functions Outside the United States (Oct 2016) (Section 862, as amended, of the National Defense Authorization Act for Fiscal Year 2008; 10 U.S.C. 2302 Note).
- 52.226-6, Promoting Excess Food Donation to Nonprofit Organizations. (Jun 2020) (42 U.S.C. 1792). Flow down required in accordance with paragraph (e) of FAR clause 52.226-6.
- 52.244-6, Subcontracts for Commercial Items (Sep 2023).
- 52.247-64, Preference for Privately Owned U.S. Flag Commercial Vessels (Nov 2021) (46 U.S.C. Appx. 1241(b) and 10 U.S.C. 2631). Flow down required in accordance with paragraph (d) of FAR clause 52.247-64.
- 18 U.S.C. § 201: Bribery of public officials and witnesses.
- The Foreign Corrupt Practices Act of 1977, as amended, 15 U.S.C. §§ 78dd-1, et seq. ("FCPA"),"
- The rights outlined in 41 U.S.C. 4712 (implemented by FAR 52.203-17, Contractor Employee Whistleblower Rights and Requirement to Inform Employees of Whistleblower Rights), 10 U.S.C. 2409 (implemented in DFARS 203.9, Whistleblower Protections for Contractor Employees), and 18 U.S.C. 1833(b) (Immunity from Liability for Confidential Disclosure of a Trade Secret to the Government or in a Court Filing).

As a supplier to Carahsoft, supplier shall affirm its status as a bona fide selling agency in accordance with FAR 3.4 and is genuinely and effectively engaged in the business of selling or leasing products or services. Further, to the extent necessary, supplier will hold valid authorizations for the representation and sale of products and services and shall adhere to ethical business practices. Supplier recognizes this is a critical aspect of partnership with Carahsoft.

SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING

Suppliers must agree to and comply with DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, when specified by a Purchase Order or subcontract from Carahsoft to Supplier. The full text of this clause is incorporated herein.

SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING (JAN 2023)

(a) *Definitions*. As used in this clause—

"Adequate security" means protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information.

"Compromise" means disclosure of information to unauthorized persons, or a violation of the security policy of a system, in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object, or the copying of information to unauthorized media may have occurred.

"Contractor attributional/proprietary information" means information that identifies the contractor(s), whether directly or indirectly, by the grouping of information that can be traced back to the contractor(s) (e.g., program description, facility locations), personally identifiable information, as well as trade secrets, commercial or financial information, or other commercially sensitive information that is not customarily shared outside of the company.

"Controlled technical information" means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information would meet the criteria, if disseminated, for distribution statements B through F using the criteria set forth in DoD Instruction 5230.24, Distribution Statements on Technical Documents. The term does not include information that is lawfully publicly available without restrictions.

"Covered contractor information system" means an unclassified information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits covered defense information.

"Covered defense information" means unclassified controlled technical information or other information, as described in the Controlled Unclassified Information (CUI) Registry at http://www.archives.gov/cui/registry/category-list.html, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies, and is—

(1) Marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of DoD in support of the performance of the contract; or

(2) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract.

"Cyber incident" means actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein.

"Forensic analysis" means the practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data.

"Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

"Malicious software" means computer software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. This definition includes a virus, worm, Trojan horse, or other code-based entity that infects a host, as well as spyware and some forms of adware.

"Media" means physical devices or writing surfaces including, but is not limited to, magnetic tapes, optical disks, magnetic disks, large-scale integration memory chips, and printouts onto which covered defense information is recorded, stored, or printed within a covered contractor information system.

''Operationally critical support'' means supplies or services designated by the Government as critical for airlift, sealift, intermodal transportation services, or logistical support that is essential to the mobilization, deployment, or sustainment of the Armed Forces in a contingency operation.

"Rapidly report" means within 72 hours of discovery of any cyber incident.

"Technical information" means technical data or computer software, as those terms are defined in the clause at DFARS 252.227-7013 , Rights in Technical Data—Other Than Commercial Products and Commercial Services, regardless of whether or not the clause is incorporated in this solicitation or contract. Examples of technical information include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.

(b) *Adequate security*. The Contractor shall provide adequate security on all covered contractor information systems. To provide adequate security, the Contractor shall implement, at a minimum, the following information security protections:

(1) For covered contractor information systems that are part of an Information Technology (IT) service or system operated on behalf of the Government, the following security requirements apply:

(i) Cloud computing services shall be subject to the security requirements specified in the clause 252.239-7010 , Cloud Computing Services, of this contract.

(ii) Any other such IT service or system (i.e., other than cloud computing) shall be subject to the security requirements specified elsewhere in this contract.

(2) For covered contractor information systems that are not part of an IT service or system operated on behalf of the Government and therefore are not subject to the security requirement specified at paragraph (b)(1) of this clause, the following security requirements apply:

(i) Except as provided in paragraph (b)(2)(ii) of this clause, the covered contractor information system shall be subject to the security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" (available via the internet at http://dx.doi.org/10.6028/NIST.SP.800-171) in effect at the time the solicitation is issued or as authorized by the Contracting Officer.

(ii)(A) The Contractor shall implement NIST SP 800-171, as soon as practical, but not later than December 31, 2017. For all contracts awarded prior to October 1, 2017, the Contractor shall notify the DoD

Chief Information Officer (CIO), via email at osd.dibcsia@mail.mil, within 30 days of contract award, of any security requirements specified by NIST SP 800-171 not implemented at the time of contract award.

(B) The Contractor shall submit requests to vary from NIST SP 800-171 in writing to the Contracting Officer, for consideration by the DoD CIO. The Contractor need not implement any security requirement adjudicated by an authorized representative of the DoD CIO to be nonapplicable or to have an alternative, but equally effective, security measure that may be implemented in its place.

(C) If the DoD CIO has previously adjudicated the contractor's requests indicating that a requirement is not applicable or that an alternative security measure is equally effective, a copy of that approval shall be provided to the Contracting Officer when requesting its recognition under this contract.

(D) If the Contractor intends to use an external cloud service provider to store, process, or transmit any covered defense information in performance of this contract, the Contractor shall require and ensure that the cloud service provider meets security requirements equivalent to those established by the Government for the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline (https://www.fedramp.gov/resources/documents/) and that the cloud service provider complies with requirements in paragraphs (c) through (g) of this clause for cyber incident reporting, malicious software, media preservation and protection, access to additional information and equipment necessary for forensic analysis, and cyber incident damage assessment.

(3) Apply other information systems security measures when the Contractor reasonably determines that information systems security measures, in addition to those identified in paragraphs (b)(1) and (2) of this clause, may be required to provide adequate security in a dynamic environment or to accommodate special circumstances (e.g., medical devices) and any individual, isolated, or temporary deficiencies based on an assessed risk or vulnerability. These measures may be addressed in a system security plan.

(c) *Cyber incident reporting requirement*.

(1) When the Contractor discovers a cyber incident that affects a covered contractor information system or the covered defense information residing therein, or that affects the contractor's ability to perform the requirements of the contract that are designated as operationally critical support and identified in the contract, the Contractor shall—

(i) Conduct a review for evidence of compromise of covered defense information, including, but not limited to, identifying compromised computers, servers, specific data, and user accounts. This review shall also include analyzing covered contractor information system(s) that were part of the cyber incident, as well as other information systems on the Contractor's network(s), that may have been accessed as a result of the incident in order to identify compromised covered defense information, or that affect the Contractor's ability to provide operationally critical support; and

(ii) Rapidly report cyber incidents to DoD at https://dibnet.dod.mil.

(2) *Cyber incident report*. The cyber incident report shall be treated as information created by or for DoD and shall include, at a minimum, the required elements at https://dibnet.dod.mil.

(3) *Medium assurance certificate requirement.*In order to report cyber incidents in accordance with this clause, the Contractor or subcontractor shall have or acquire a DoD-approved medium assurance certificate to report cyber incidents. For information on obtaining a DoD-approved medium assurance certificate, see https://public.cyber.mil/eca/.

(d) *Malicious software.* When the Contractor or subcontractors discover and isolate malicious software in connection with a reported cyber incident, submit the malicious software to DoD Cyber Crime Center (DC3) in accordance with instructions provided by DC3 or the Contracting Officer. Do not send the malicious software to the Contracting Officer.

(e) *Media preservation and protection*. When a Contractor discovers a cyber incident has occurred, the Contractor shall preserve and protect images of all known affected information systems identified in paragraph (c)(1)(i) of this clause and all relevant monitoring/packet capture data for at least 90 days from the submission of the cyber incident report to allow DoD to request the media or decline interest.

(f) *Access to additional information or equipment necessary for forensic analysis.*Upon request by DoD, the Contractor shall provide DoD with access to additional information or equipment that is necessary to conduct a forensic analysis.

(g) *Cyber incident damage assessment activities*. If DoD elects to conduct a damage assessment, the Contracting Officer will request that the Contractor provide all of the damage assessment information gathered in accordance with paragraph (e) of this clause.

(h) *DoD safeguarding and use of contractor attributional/proprietary information.* The Government shall protect against the unauthorized use or release of information obtained from the contractor (or derived from information obtained from the contractor) under this clause that includes contractor attributional/proprietary information, including such information submitted in accordance with paragraph (c). To the maximum extent practicable, the Contractor shall identify and mark attributional/proprietary information. In making an authorized release of such information, the Government will implement appropriate procedures to minimize the contractor attributional/proprietary information that is included in such authorized release, seeking to include only that information that is necessary for the authorized purpose(s) for which the information is being released.

(i) *Use and release of contractor attributional/proprietary information not created by or for DoD.* Information that is obtained from the contractor (or derived from information obtained from the contractor) under this clause that is not created by or for DoD is authorized to be released outside of DoD—

(1) To entities with missions that may be affected by such information;

(2) To entities that may be called upon to assist in the diagnosis, detection, or mitigation of cyber incidents;

(3) To Government entities that conduct counterintelligence or law enforcement investigations;

(4) For national security purposes, including cyber situational awareness and defense purposes (including with Defense Industrial Base (DIB) participants in the program at 32 CFR part 236); or

(5) To a support services contractor (“recipient”) that is directly supporting Government activities under a contract that includes the clause at 252.204-7009 , Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information.

(j) *Use and release of contractor attributional/proprietary information created by or for DoD.* Information that is obtained from the contractor (or derived from information obtained from the contractor) under this clause that is created by or for DoD (including the information submitted pursuant to paragraph (c) of this clause) is authorized to be used and released outside of DoD for purposes and activities authorized by

paragraph (i) of this clause, and for any other lawful Government purpose or activity, subject to all applicable statutory, regulatory, and policy based restrictions on the Government's use and release of such information.

(k) The Contractor shall conduct activities under this clause in accordance with applicable laws and regulations on the interception, monitoring, access, use, and disclosure of electronic communications and data.

(l) *Other safeguarding or reporting requirements.* The safeguarding and cyber incident reporting required by this clause in no way abrogates the Contractor's responsibility for other safeguarding or cyber incident reporting pertaining to its unclassified information systems as required by other applicable clauses of this contract, or as a result of other applicable U.S. Government statutory or regulatory requirements.

(m) *Subcontracts*. The Contractor shall—

(1) Include this clause, including this paragraph (m), in subcontracts, or similar contractual instruments, for operationally critical support, or for which subcontract performance will involve covered defense information, including subcontracts for commercial products or commercial services, without alteration, except to identify the parties. The Contractor shall determine if the information required for subcontractor performance retains its identity as covered defense information and will require protection under this clause, and, if necessary, consult with the Contracting Officer; and

(2) Require subcontractors to—

(i) Notify the prime Contractor (or next higher-tier subcontractor) when submitting a request to vary from a NIST SP 800-171 security requirement to the Contracting Officer, in accordance with paragraph (b)(2)(ii)(B) of this clause; and

(ii) Provide the incident report number, automatically assigned by DoD, to the prime Contractor (or next higher-tier subcontractor) as soon as practicable, when reporting a cyber incident to DoD as required in paragraph (c) of this clause.

(End of clause)

DPAS RATING

If there is a priority rating on a Purchase Order issued to Supplier by Carahsoft, then in accordance with FAR 52.211-15 it is a rated Purchase Order certified for national defense, emergency preparedness, and program use, and Suppliers shall follow all requirements of the Defense Priorities and Allocations System (DPAS) regulation (15 CFR 700). By acceptance of this Purchase Order, Supplier agrees to process this Purchase Order in accordance with the above criteria. Supplier performance or delivery under the applicable Purchase Order further constitutes Supplier acknowledgment of, and agreement to, the DPAS regulation.

ADHERENCE TO LABOR LAW, EMPLOEE RIGHTS AND PROTECTIONS

Policies should be in place to confirm the Supplier's commitment to these points and improvement programs should be in place where relevant:

Wages and benefits: At a minimum, the legal minimum wage standard must be adhered to across the entire workforce, employees should receive clear information on their wages, and unfair deductions from wages as a disciplinary measure are not permitted.

Working hours: Working hours must be limited according to national or local law, including breaks.

Overtime should be voluntary, should not replace regular employment and must be fairly compensated.

Freedom of association, collective bargaining or parallel means: Employees have the right to join or form a trade union without facing discrimination or intimidation. Where freedom of association and collective bargaining is restricted under law, employees should have the right to develop parallel means.

Health and safety and working conditions: A safe and hygienic working environment should be provided with an awareness of any industry-specific hazards. Relevant training should be provided to employees.

Regular employment: All employees should be provided with a written employment contract setting out

SUBCONTRACTING

Where authorized subcontracting is used by Supplier to support the execution of services for Carahsoft, Supplier shall confirm that the subcontractor meets the minimum expectations set out in this Section through the following controls:

A. Supplier shall take necessary steps to obtain and maintain visibility over labor rights and risks within the operations and supply chains of subcontractors;
B. Supplier shall attain the right to audit over subcontractor operations; and
C. Records of audits undertaken of subcontractors shall be available on request.

Supplier shall have written agreements in place with subcontractors to ensure that any further subcontracting by the subcontractor company (a) is authorized and (b) meets the standards set out in this document.

DIVERSITY AND INCLUSIVENESS

Suppliers will be required to comply with any applicable discrimination legislation. Our Suppliers will be treated fairly and equally during the tendering and purchasing process, with decisions made on the basis of clear selection criteria.

Carahsoft expects Suppliers to have a policy in place to consider usability by, and inclusion of, individuals with disabilities when designing products and/or delivering services to Carahsoft. As part of the policy, there are accessibility standards and/or processes in place that conform to disability guidelines when Suppliers are designing products and/or delivering services.

Carahsoft expects Suppliers to have a policy that explicitly bans discrimination/bullying and harassment based on sexual orientation, race, gender or gender identity/expression. In addition, Suppliers are also encouraged to have evidence of diversity and inclusiveness training that is inclusive of sexual orientation and gender Identity/expression.

Our Inclusive Procurement strategy's chief objective is to identify, develop and utilize certified diverse businesses (defined below) that can enhance our competitive advantage and provide innovative and cost-effective products and services for us and our clients. It is our expectation that all Suppliers use their best efforts themselves to procure diverse businesses to compete for goods and services to become preferred Suppliers to the Supplier and/or as its subcontractor(s). In accordance with the terms of its agreement with Carahsoft, Suppliers commit to comply with all relevant regulatory agency requirements, as well as with any local diversity regulations and programs.

For the purposes of this Supplier Code of Conduct, a "diverse business" is a company that is certified to be

at least 51%-owned, -operated and -controlled by one or more minority, woman, LGBT+ person, person with a disability, veteran, service-disabled veteran, or aboriginal or indigenous person. In addition, historically underutilized business and social enterprises as defined by the local country will be included in the diverse business classification.

It is our commitment that diverse business enterprises shall have equal opportunity to compete for all goods and services to become preferred Suppliers and/or subcontractor(s) for the organization. Carahsoft is committed to the development and growth of diverse business enterprises to build a better working world and to expand networks to build trusted and enriched relationships.

Carahsoft expects Suppliers to have equivalent policies to promote diversity in their supply chains and purchase from diverse businesses. Suppliers agree to make a reasonable effort to utilize diverse suppliers and provide evidence to Carahsoft upon request.

MONITORING

Carahsoft may conduct annual compliance surveys to confirm compliance with this Supplier Code of Conduct. However, Carahsoft expects that Suppliers will actively audit and monitor their day-to-day management processes with respect to the Carahsoft Code of Conduct and provide evidence to Carahsoft upon request. All costs associated with the annual compliance survey will be the responsibility of Carahsoft.

