

**AGREEMENT FOR CONSULTING SERVICES PERTAINING TO NETWORK SECURITY
ASSESSMENT**

This Agreement for Consulting Services ("Agreement") is made and effective as of June 13, 2022, by and between the State Board of Administration of Florida (the "SBA"), located at 1801 Hermitage Boulevard, Tallahassee, Florida 32308, and Peraton State & Local Inc. (the "Consultant"), located at 15050 Conference Center Drive, Chantilly, Virginia 20151.

WITNESSETH

For good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the SBA hereby retains and engages the Consultant to act on the terms and conditions hereinafter set forth.

I. SERVICES TO BE PROVIDED

The Consultant shall provide certain consulting services pertaining to a network security assessment for the SBA. The Services to be provided are more particularly set forth in Schedule A, attached hereto and by this reference made a part of this Agreement.

In addition, the SBA may ask Consultant to provide additional consulting and other non-retainer services (hereinafter "Additional Services") as the SBA may require during the term of the Agreement. The scope and nature of such Additional Services will be negotiated by the parties as needed.

II. TERMS AND CONDITIONS:

A. Term of Contract:

This Agreement shall have an initial term of five (5) years, commencing as of the date first written above. The term of the Agreement may be extended for five (5) additional one-year periods, upon the mutual written agreement of the parties.

Notwithstanding the foregoing, either party may terminate this Agreement upon written notice under the terms and conditions of the Agreement.

B. Fee Schedule:

1. As compensation for the Services, the SBA shall pay to the Consultant the following fees:

	<u>Fees*</u>	Total Not to Exceed <u>Hours</u>
Year 1	\$ 102,710	460
Year 2	\$ 87,851	380

Year 3	\$ 105,197	460
Year 4	\$ 92,479	380
Year 5	<u>\$ 109,488</u>	<u>460</u>
Total for all Five Years	\$ 497,725	2,140

*Pricing is all inclusive of hardware, licenses, travel and incidentals required to support the SBA during the course of the assessments during the five (5) year period.

2. If additional hours are needed beyond what is proposed, the hourly rate by resource is at \$235 per hour.
3. Consultant will select and provide all software licenses and tools used in performing the network security assessments.
4. Services will be invoiced monthly as Time and Materials.

C. Key Personnel:

Consultant shall determine which of its personnel shall be assigned to perform the Services under this Agreement and reserves the right to replace or reassign such personnel during the term hereof; provided, however, that Consultant shall, subject to scheduling and staffing considerations, use commercially reasonable efforts to honor SBA's request for specific individuals for performing the Services. In addition, at any time during the term of this Agreement, Consultant shall provide the SBA with written notification of changes in Key Personnel (as hereinafter defined), or to the duties to be performed by such personnel, at least two (2) weeks in advance of any such changes. Notwithstanding the foregoing, in the event that Consultant experiences changes in Key Personnel which take effect less than two (2) weeks after the Consultant's President becomes aware that such change will occur, the Consultant shall notify the SBA of such changes within two (2) business days from the date on which the Consultant's President becomes aware of such change. In the event that such notification is provided during such period, the terms of this Agreement shall be deemed to have been satisfied, notwithstanding that two (2) weeks' notice was not provided. For purposes of this Agreement, the Key Personnel initially shall be Patrick Hogan and Andrea Wood. Thereafter, the Key Personnel shall include any of replacements as reasonably approved by the SBA under this Section II(C) (The "Key Personnel"). This Agreement may be terminated in accordance with Section II(J) hereof upon written notice from the SBA to Consultant because of changes in the Key Personnel not made in accordance with the immediately preceding two sentences or otherwise. SBA will also have full access to any personnel, other than the Key Personnel, that produce work product or recommendations under the terms of this Agreement; (e.g., policy or research committees and their members).

D. Confidentiality

1. Consultant, in the course of its duties, will have access to certain non-public information pertaining to the FRS Defined Benefit Plan, the FRS Defined Contribution Plan, other SBA mandates, the SBA and its employees, and/or the State of Florida. All such information may be confidential, pursuant to the provisions Florida law, including, without limitation, Sections 215.4401, 215.557, and 121.4501(19), Florida Statutes. Consultant agrees that all confidential information shall be received in strict confidence and shall be used only for the purposes of this Agreement. Consultant further agrees that such confidential information shall only be provided to parties, whether internal or external to Consultant, that are directly involved with performing the duties under the Agreement and that further have a need to know the confidential information in order to carry out their duties in support of the Agreement. Consultant agrees to take all reasonable precautions to prevent the disclosure of such information to parties other than those previously specified except as may be necessary by reason of legal (including the provisions of Chapter 119, Florida Statutes), accounting or regulatory requirements, as the case may be. The obligation to treat information as confidential shall not apply to information which:
 - a) is in the public domain, other than by any breach of this Agreement;
 - b) is in the possession of the Consultant on the effective date of this Agreement, and such information was not obtained from the SBA;
 - c) was developed by Consultant outside the scope of any agreement with the SBA; or
 - d) was obtained rightfully from third parties.
2. Consultant shall treat the confidential information as confidential, using the same standard of care that it uses to protect its own proprietary or confidential information (but not less than a reasonable standard of care), and no information shall be disclosed to third parties by the Consultant, its officers, employees, consultants, or agents without the prior written request of the SBA. Consultant agrees to take all reasonable precautions to prevent the disclosure to third parties of such information, except as may be necessary by reason of legal, accounting or regulatory requirements, as the case may be.
3. Consultant shall not be bound by this Section to the extent that it acts under compulsion of law or in accordance with the requirements of any national or local government instrumentality. If Consultant is required to disclose confidential information pursuant to such requirements of law, the Consultant shall first notify the SBA so that it may seek protective orders or take any other legal action it deems necessary. Any Confidential Information disclosed pursuant to requirements of law shall still be deemed confidential.
4. The SBA and the Consultant acknowledge and agree that a breach of these confidentiality obligations would cause irreparable harm to the SBA and that no adequate remedy is available at law for such breach. Accordingly, it is agreed that the SBA will be entitled to an injunction or injunctions to prevent breaches of these confidentiality obligations and to enforce specifically the terms and provisions of this Section II(D).

E. Conflict of Interest

1. Consultant shall not directly or indirectly receive any benefit from recommendations made to the SBA and shall disclose to the SBA any actual or potential personal investment or economic interest of the Consultant or, to its knowledge, any officer, director or employee thereof which may be enhanced by the recommendations made to the SBA. Consultant acknowledges and understands that the SBA is subject to the provisions of Chapter 112, Part III, "Code of Ethics for Public Officers and Employees," Florida Statutes, and all rules adopted thereunder, and Consultant agrees to comply promptly with any requirements that may be applicable to it thereunder. Consultant represents that it and/or its parent organization currently has, and further covenants that it and/or its parent organization will have at all times during the term of this Agreement, a code of ethics, code of professional conduct or other policies and procedures that prohibit all officers, directors or employees thereof from engaging in any activity or conduct that would constitute an actual or perceived conflict of interest between such person and the Consultant's clients without the prior written approval of Consultant.
2. Consultant shall promptly notify the SBA of any pending or threatened action by Consultant's clients regarding the retention of Consultant based on any allegation of an actual or perceived conflict of interest between such client and Consultant (including any divisions, subsidiaries or affiliates).

F. Indemnification

Consultant shall indemnify and hold the SBA, its Trustees, officers and employees harmless from any and all losses, costs, claims, damages, liabilities, judgments, actions, costs and expenses (including reasonable attorneys' fees), resulting from or arising out of negligence, omissions, fraud, willful misconduct or breach of duty or this contract (including all Addenda); or Consultant's breach of data security; or the violation of or non-compliance with any law, rule, regulation or other legal requirement (including without limitation, the securities laws) of Consultant or its agents, nominees, appointees or subcontractors.

G. Compliance with Laws.

The Consultant hereby covenants and agrees that at all times during the term of this Agreement, the Consultant shall comply with all applicable laws, rules, regulations, industry/professional standards, or other applicable legal requirements (including, without limitation, all applicable laws, rules, regulations, and industry standards relating to cybersecurity or data collection, storage, security or privacy) to which the Consultant, its Services or any of the activities contemplated by this Agreement are subject.

H. Public Records

1. Notwithstanding any provision in this Agreement between the parties, Consultant acknowledges and agrees that the SBA is bound by the provisions of Chapter 119 (Public Records), Florida Statutes, and in the event of any conflict between Chapter 119, Florida Statutes, and the terms of this Agreement between the parties, the provisions and procedures of Chapter 119, Florida Statutes, shall prevail. To the extent applicable, Consultant shall comply with Chapter 119, Florida Statutes. In particular, Consultant shall:
 - (a) Keep and maintain public records required by the SBA in order to perform the Services under this Agreement;
 - (b) Upon request from the SBA's custodian of public records, provide the SBA with a copy of the requested public records or allow such records to be inspected or copied within a reasonable time at a cost that does not exceed the cost provided in Chapter 119, Florida Statutes or as otherwise provided by Florida law;
 - (c) Ensure that public records that are exempt or confidential and exempt from public records disclosure requirements are not disclosed except as authorized by law for the duration of the contract term and following the completion of the contract if Consultant does not transfer the records to the SBA when the Agreement is completed;
 - (d) Upon completion of the Agreement, transfer, at no cost, to the SBA all public records in Consultant's possession or keep and maintain the public records required by the SBA in order to perform the services under this Agreement. If Consultant transfers all public records to the SBA upon completion of the contract, Consultant shall destroy any duplicate public records that are exempt or confidential and exempt from public records disclosure requirements. If Consultant keeps and maintains public records upon completion of the contract, Consultant shall meet all applicable requirements for retaining public records. Consultant shall, upon request from the SBA's custodian of records, provide all records that are stored electronically to the SBA in a format that is compatible with the information technology systems of the SBA.
 - (e) IF CONSULTANT HAS QUESTIONS REGARDING THE APPLICATION OF CHAPTER 119, FLORIDA STATUTES, TO CONSULTANT'S DUTY TO PROVIDE PUBLIC RECORDS RELATING TO THIS CONTRACT, CONTACT THE SBA'S CUSTODIAN OF PUBLIC RECORDS AT: STATE BOARD OF ADMINISTRATION OF FLORIDA, POST OFFICE BOX 13300, TALLAHASSEE, FLORIDA 32317-3300, sbacontracts@sbafla.com, (850) 488-4406.

(f) Consultant consents and agrees to be sued in, and subject to the exclusive jurisdiction of, Florida state courts located in Leon County, Florida with respect to any civil or criminal litigation required to enforce the provisions of Chapter 119, Florida Statutes, or the provisions of this Section II.(H).

(g) All requests, including telephone requests, for inspection of public records shall be immediately forwarded to the SBA's Office of General Counsel.

I. Right to Audit

(a) During the term of and for a period of five (5) years after the expiration or termination of the Agreement, the SBA shall have the right to have any person or entity designated by the SBA, including an independent public accountant or auditor and/or any federal or state auditor, to inspect, review and/or audit, any books, records and supporting documents relating to the Agreement and/or the subject matter of the Agreement (the "Records"). In the event such right is exercised and upon no less than ten (10) business days' prior written notice by the SBA, Consultant agrees to permit reasonable access to its premises and the Records during Consultant's normal business hours. The SBA shall have the right, in connection with any such inspection, review and/or audit, to have one or more members of its staff present at all times. During the term of and for a period of five (5) years after the expiration or termination of the Agreement (or for any longer period of time that may be required by any applicable law relating to the retention of Records), Consultant shall maintain and retain the Records, at its sole expense. In the event the SBA and/or its designees are in the process of conducting such an inspection, review and/or audit upon the expiration of the five (5)-year access and/or retention periods described herein, then this Section II.(I). shall survive in its entirety until the conclusion of such inspection, review and/or audit, in the SBA's or the SBA designee's reasonable determination. For the avoidance of doubt, the scope of any inspection, review and/or audit under this Section may include, without limitation, Consultant's compliance with the terms of the Agreement.

(b) Consultant shall use best efforts to cooperate with the SBA and any person or entity designated by the SBA in connection with any inspection, review and/or audit under this Section including, without limitation, causing its relevant and knowledgeable employees and/or representatives to be available to assist and to respond to reasonable inquiries and requests of the SBA and/or its designees. Consultant shall respond (including, if relevant and appropriate, with an action plan) within a reasonable time to any reports, findings and/or assessments provided to Consultant by the SBA and/or its designees, and Consultant shall provide a copy of all such responses to the SBA (including the SBA's management contact listed in the Letter of Understanding. Consultant acknowledges and agrees that any such report, finding and/or assessment is intended for the sole use and for the benefit of the SBA.

(c) Except as set forth herein, the SBA shall bear the costs of any inspection, review and/or audit described in this Section II.(I). However, in the event Consultant engaged in

or committed (including through acts or omissions) any fraud, misrepresentation and/or non-performance, then Consultant shall be obligated to reimburse the SBA for the total costs of inspection, review and/or audit. Consultant's reimbursement obligation herein shall be in addition to all other rights, remedies and damages available to the SBA at law or in equity, which shall not be deemed waived or relinquished in any way because of Consultant's additional reimbursement obligation hereunder.

J. Termination:

The SBA may terminate the Agreement at any time for any reason whatsoever upon providing thirty (30) days written notice to the Consultant. The Consultant may resign upon sixty (60) days advance written notice. However, certain provisions of the Agreement may survive the termination of the Agreement by the SBA or the resignation of the Consultant under the Agreement. Except as set forth herein or as otherwise required by law, upon expiration or termination hereof, Consultant shall have no further obligations under this Agreement. As long as the SBA is not in material breach of its obligations under this Agreement, Consultant shall continue to serve, at the same fees, at the SBA's request until the appointment of a successor.

K. Assignments

Consultant shall not assign or delegate its rights or responsibilities without the prior written consent of the SBA. No person or organization may succeed to or assume Consultant's rights and obligations under the Agreement by operation of law, whether by merger, consolidation, change in control, reorganization or otherwise without the SBA's prior written consent.

L. Subcontractors/Agents

Consultant shall be responsible and accountable for the acts or omissions of Consultant Representatives (including the Consultant's officers, directors, employees, agents, contractors, subcontractors and consultants, including affiliates thereof) to the same extent it is responsible and accountable for its own actions or omissions under the Agreement. Consultant agrees to impose the requirements of this Agreement on all Contractor Representatives. Consultant shall execute a written agreement with each Consultant Representative containing equivalent terms to this Agreement.

M. Information to be Provided

Consultant shall assume any information the SBA supplies (or which is supplied on its behalf) is accurate and complete. Consultant's responsibilities (and the associated project fees) do not include extensive independent verification of required information.

N. Consultant Intellectual Capital

Consultant hereby grants to the SBA and its successors and assigns a perpetual license to use, alter and modify for any purpose any and all work, services (including the Services), records, information, methodologies, processes, documentation, deliverables or any other intellectual capital of any kind, including all modifications, derivations and adaptations thereof (the "Intellectual Capital"), performed, prepared, created or developed, in whole or in part, by the Consultant under this Agreement, subject to the understanding that the SBA shall not sell or transmit the Intellectual Capital to third persons for compensation (which shall exclude reimbursement or payment for copying and other ministerial costs) unless otherwise required by law. Except as otherwise set forth above, Consultant shall retain exclusive rights to the Intellectual Capital. Notwithstanding the foregoing, the Consultant, for itself and its past, present and future successors, assigns, representatives, officers, directors, shareholders, employees and agents, does hereby release, permit, acquit, satisfy, and forever discharge the SBA, its successors, assigns, affiliates, trustees, officers, and employees from any and all claims, demands, actions, causes of action, costs, expenses, attorneys' fees, sums of money, lost profits, damages and all liabilities of any kind whatsoever (the "Liabilities"), at law or in equity, whether known or unknown, that Consultant had, now has and may have in the future relating to the SBA's use, transmission and disclosure of the Intellectual Capital, except for the Liabilities directly resulting from the SBA's material breach of this Section II.(N).

O. Governing Law and Jurisdiction

This Agreement shall be governed by, construed under and interpreted in accordance with laws of the State of Florida without regard to conflict of law principles. Any proceedings to resolve disputes regarding or arising out of this Agreement shall be conducted in the state courts located in Leon County, Florida, and the parties hereby consent to the jurisdiction and venue of those courts.

P. E-Verify.

Consultant acknowledges that the SBA is subject to, and Consultant agrees to comply with Section 448.095, Florida Statutes, to the extent applicable.

Q. Agreement Transparency.

Consistent with the Florida Transparency in Contracting Initiative, the SBA posts certain operational Agreements on its website, and this Agreement will be one of the agreements posted. Consultant hereby agrees that the SBA is authorized to post this Agreement (including any amendments or addenda hereto) and a description of the content of the Agreement (including any amendments or addenda hereto) on the SBA's website.

R. Former SBA Employees

Except upon the prior written approval of the SBA, Consultant shall not assign any former employee of the SBA to perform any of the services in this Agreement.

S. Data Security

Consultant and the SBA agree to the terms set forth in Schedule B, the Data Security Terms and the Systems Use Agreement, which are attached hereto and incorporated into this Agreement by this reference.

T. Counterparts

This Agreement may be executed in one or more counterparts, and when each party has executed at least one counterpart, this Agreement shall be deemed to be one and the same document.

U. Severability

If one or more provisions of this Agreement or the application of any such provisions to any set of circumstances shall be determined to be invalid or ineffective for any reason, such determination shall not affect the validity and enforceability of the remaining provisions or the application of the same provisions or any of the remaining provisions to other circumstances.

V. Remedies

All rights and remedies granted under this Agreement shall be cumulative and not exclusive of any other rights and remedies which the parties may have at law or in equity. The parties may exercise all or any of such rights and remedies at any one or more times without being deemed to have waived any or all other rights or remedies which they may have.

W. Survival

All representations, warranties, covenants and agreements set forth in Section II(F), (G), (H), (I), (J), (N), (O), (P), (R), (S), (V) and (Y) of this Agreement or in any instrument, document, agreement or writing delivered in connection therewith shall survive the completion of any of the Services provided hereunder or the termination of this Agreement.

X. Entire Agreement

The SBA and Consultant acknowledge that they have read this Agreement and that together with all written amendments, exhibits, schedules, and addenda hereto, which shall be incorporated by reference herein, this Agreement constitutes the entire and exclusive agreement between the SBA and Consultant with respect to the subject matter hereof, and no statement, agreement, or understanding not contained herein shall be

enforced or recognized. THIS AGREEMENT CANNOT BE MODIFIED OR SUPPLEMENTED BY ORAL STATEMENTS MADE EITHER BEFORE OR AFTER EXECUTION OF THIS AGREEMENT AND ANY SUCH STATEMENTS DO NOT CONSTITUTE WARRANTIES. NO COLLATERAL OR PRIOR STATEMENTS, REPRESENTATIONS, UNDERSTANDINGS, AGREEMENTS, OR WARRANTIES (EXPRESS OR IMPLIED) ARE A PART OF THIS AGREEMENT.

Y. Binding Effect

This Agreement shall be binding upon the parties, their successors, legal representatives, and assignees. Consultant and SBA intend this Agreement to be a valid legal instrument, and no provision of this Agreement which shall be deemed unenforceable shall in any way invalidate any other provision of this Agreement, all of which remain in full force and effect. No waiver, alteration, or modification of any of the provisions of this Agreement shall be effective or binding unless in writing and signed by authorized representatives of both parties.

Z. Relationship of the Parties

The relationship between the parties is that of independent contractors. None of the provisions of this Agreement shall be construed to create a partnership or joint venture relationship between the parties or the partners, officers, members or employees of the other party by virtue of either this Agreement or actions taken pursuant to this Agreement. No employee or representative of Consultant will hold himself or herself out as, nor claim to be, an officer or employee of the State or the SBA by reason of this Agreement, nor will he or she make any claim of right, privilege or benefit which would accrue to an employee of the SBA under Florida law.

aa. SBA Policies

Communication Policy. Consultant acknowledges and agrees that it has received the SBA Communications Policy (#10-004) (the "Communications Policy"). Consultant covenants and agrees that it shall comply with the Communication Policy, and such modifications to the policy as may be provided to Consultant from time to time, to the fullest extent that the Communications Policy applies to the Consultant. Consultant may not identify the SBA for purposes of business development or press releases without the express prior written consent of the SBA.

Fraud Hotline. The SBA maintains a fraud hotline at (888) 876-7548 to encourage individuals to report suspected SBA-related fraud, theft, or financial misconduct on an anonymous basis. Within 30 days following the effective date of this Agreement, Consultant agrees to communicate this hotline information to those of its employees that are responsible for providing services under this contract. Consultant also agrees to re-communicate this hotline information at the request of the SBA.

bb. Notices

All notices, requests, instructions, other advice, or documents required hereunder shall be in writing and delivered personally or via a recognized overnight delivery service mailed by first-class mail, postage prepaid, to the following:

If to the SBA:

if mailed: State Board of Administration of Florida
Post Office Box 13300
Tallahassee, Florida 32317-3300
Attention: Executive Director

if hand delivered: State Board of Administration of Florida
1801 Hermitage Boulevard
Suite 100
Tallahassee, Florida 32308
Attention: Executive Director

If to the Consultant: Peraton State & Local Inc.
15050 Conference Center Drive
Chantilly, Virginia 20151
Attention: Joan M. Galvin, Contract Administrator
Email: joan.m.galvin@mail.peraton.com

Peraton State & Local Inc.
15050 Conference Center Drive
Chantilly, Virginia 20151
Attention: Ernie Sanders, Director
Email: ernie.sanders@mail.peraton.com

cc. No Waiver:

A party's failure at any time to enforce any of the provisions of this Agreement or any right with respect thereto shall not be construed to be a waiver of such provision or right, nor to affect the validity of this Agreement. The exercise or non-exercise by a party of any right under the terms or covenants herein shall not preclude or prejudice the exercising thereafter of the same or other rights under this Agreement.

dd. Nondiscrimination:

Consultant agrees not to discriminate against any employee or applicant because of age, race, religion, color, handicap, sex, physical conditions, developmental disability, sexual orientation or national origin.

ee. Headings and Captions.

All headings and captions contained in this Agreement are for convenience of reference only and shall not affect in any way the interpretation or meaning of this Agreement.

ff. Pronouns.

Words used herein, regardless of the number and gender specifically used, shall be deemed and construed to include any other number, singular or plural, and any other gender, masculine, feminine, or neuter, as the context requires.

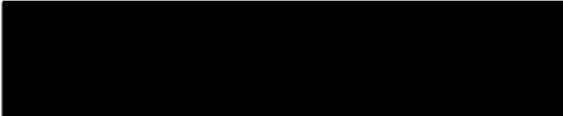
gg. Data Security.

Consultant and the SBA agree to the terms set forth in Schedule B, the Data Security Addendum, and the Systems Use Agreement that are attached hereto and incorporated into this Agreement by this reference.


IN WITNESS WHEREOF, the parties have caused this Agreement to be executed by their respective duly authorized officers as of the dates set forth below.

PERATON STATE & LOCAL INC.

STATE BOARD OF ADMINISTRATION
OF FLORIDA


Title: Contract Administrator


Interim ~~E~~xecutive Director & CIO



SCHEDULE A

SCOPE OF CONSULTING SERVICES

The work to be performed consists of: (1) External Network Assessments and Testing, to identify external network vulnerability and to perform non-intrusive penetration testing; and (2) Internal Network Assessments and Testing to be performed per the SBA-designated IP address ranges to identify weak points. Testing will be conducted both remotely and on-site.

Rules of Engagement (ROE) will be established prior to any testing to ensure minimal impact on operations while still maximizing the usefulness of the testing results. The ROE will be provided in writing to the SBA for review and agreement.

Consultant will perform the assessments using a four-phase process, detailed below, comprised of Pre-Testing, Passive Testing, Active Testing and Post Testing. Pre-Testing is critical for setting up the rules of engagement and scope of work. Passive and Active Testing will be the actual Penetration and Vulnerability work. The Post Test will consist of the creation of a detailed report of findings and remediation recommendations required by the SBA.

I. Testing and Assessment:

A. Pre-Testing Phase:

Consultant will develop a scope of work statement describing the target networks, devices, and applications. Questions and missing information will be identified for discussion with the SBA during the kick-off meeting. At this point, the initial project plan and schedule will be created.

Consultant's testing team will coordinate with the SBA to determine the network addresses and applications authorized for testing before proceeding with any active testing or vulnerability scanning.

Consultant will lead an introductory meeting among all relevant parties to review the testing process, coordinate required access, identify technical points of contact, solicit questions and concerns, and review the Consultant's assessment checklist.

Connectivity Testing: Consultant will validate connections to the identified networks, devices, and applications tested.

B. Passive Testing Phase:

Information Gathering / Passive Reconnaissance: Consultant will conduct a thorough investigation into open-source information to identify available data that may assist an attacker in compromising the in-scope systems and applications.

Example Passive Reconnaissance Activities Include: Server enumeration via DNS forward and reverse queries; Search engine requests; LinkedIn and Social Media searches.

Threat Modeling: Consultant may conduct threat modeling, a structured approach for identifying, quantifying, and prioritizing the risk associated with potential attack vectors relevant to an enterprise's network(s), device(s), and application(s). This provides the Consultant with a comprehensive understanding of the attack surface of the target and provides a means for organizing and prioritizing testing.

C. Active Testing Phase:

Individual Server/Host/Device Discovery: Consultant will validate known targets and identified unspecified devices that are within the scope. Consultant will identify all in-scope devices and investigate the communication services, operating systems, and functionalities associated with them.

Examples of Discovery Techniques Used During Black Box Penetration Testing Include: Reverse DNS lookups, ICMP scanning, and scanning for the most common TCP and UDP ports. When an IP is identified as live, then additional port scanning will be performed to identify the system characteristics and services available.

Web Application / Database Discovery: Where web applications are detected, Consultant may conduct detailed reviews of the target application(s) and supporting database(s), identifying installed components and versions, and mirroring/reviewing web application code and static files.

Automated Vulnerability Scanning: Consultant will use automated tools to probe the specified servers and networks. The tools will be capable of scanning for security vulnerabilities, viruses, known software bugs, configuration problems, and unnecessary services. The automated vulnerability scanning tools identify the majority of well-known vulnerabilities and information leaks and cover a wide range of problems found in web applications. The Consultant maintains a central database of publicly known vulnerabilities and uses this repository of knowledge to customize scans by defining the policies of known vulnerabilities according to the customer's IT environments.

Penetration Testing: Consultant will access the application, systems, and attempt to identify and exploit vulnerabilities using manual and semi-automated testing tools and methods. Servers and network devices vulnerability classes include, but are not limited to: Default Credentials, Remote Code Execution Vulnerabilities (e.g., network buffer overflows), and Insecure Services. In an application penetration test, vulnerability classes include, but are not limited to: Cross-Site Scripting (XSS), Cross-Site; Request Forgery (CRSF), SQL Injection, Local and Remote File Inclusion (LFI/RFI), as well as Business Logic Flaws.

Validation Testing: Consultant will use non-invasive manual validation testing to verify automated vulnerability scan results. Consultant will take a precautionary step in accordance with industry practices during this phase of service to minimize the chances of adversely affecting SBA applications, servers, and network devices. These steps include disabling denial of service attacks, brute force password guessing, or exploits known to crash or impact systems.

Escalation: Where system access is gained during the external penetration testing, Consultant will attempt to escalate privilege using a combination of known vulnerabilities, system misconfigurations, and other weaknesses.

D. Post Testing Phase:

Data Correlation and Analysis: The consolidated results from vulnerability scans, penetration tests, and validation tests will be used to identify and assist in prioritizing threats for remediation planning. Prioritization of security findings is conducted using a severity rating based on a four-tier rating system where each finding is assigned a severity rating of Exposure (high risk), Concern (medium risk), Shortcoming (low risk) or Remark.

Reporting: Consultant will provide the SBA with a final report documenting the findings, which may include the identification of any of the following: networks, devices and hosts; operating systems, services and applications; architectural designs and associated defects; vulnerabilities; evidence of validation; and recommendations for mitigation. Consultant will provide clear and concise explanations of all findings, and whenever available, easy-to-follow mitigation procedures.

Out Briefing: Consultant will present the final report, discuss specific findings, and answer any questions the SBA may have.

II. Schedule:

In years one (1), three (3), and five (5) an assessment engagement consisting of 460 hours per year will be made, with a mutually agreed upon duration. This assessment will be staffed with two full time security testers (200 hours each), a partial full time equivalent (FTE) security lead (20 hours), and a partial FTE project manager (40 hours).

In years two (2) and four (4) an assessment engagement consisting of 380 hours per year will be made, with a mutually agreed upon duration. This assessment will be staffed with two full time security testers (160 hours each), a partial FTE security lead (20 hours), and a partial FTE project manager (40 hours).

At project start, Consultant's Project Manager will work with the designated SBA point of contact to refine the scope of the project, project plan, work structure and effort committed to each authorized task. Consultant will conduct a project scope definition which include its proprietary process of identifying the specific tasks to be performed, within a testing iteration, which will be documented in a Cybersecurity Assessment Plan.

Consultant expects the project plan and activity dates will need to be flexible throughout the performance in consideration of the availability of SBA personnel. Consultant's Project Manager and the SBA Project Manager will actively manage the schedule throughout the project. Consultant's Project Manager and select Consultant team members will participate in brief weekly status conference calls with the SBA during the delivery of the authorized services to review progress, upcoming planned activities, and issues.

III. External Network Assessments and Testing – External Network Vulnerability Assessment and Penetration Testing:

Consultant will perform external penetration assessment of the SBA's corporate network in an attempt to identify vulnerabilities that are visible from the internet. Consultant will perform tests identifying IP range information through publicly available resources or by targeting ranges provided by the SBA.

Consultant will conduct a black box web application penetration test from an external adversary perspective using public (Internet)-facing entry points identified by the SBA.

An offsite "External" adversary discovers and exploits weaknesses in the SBA business applications that lead to unauthorized access with elevated privileges or obtaining access to sensitive data such as Customer Data or Intellectual Property.

The focus of the application testing is to validate security controls and discover security weaknesses, including but not limited to the Open Web Application Security Project (OWASP) Top 10 Most Critical Web Application Security Risks, through a combination of hand-crafted and automated testing.

Consultant will provide the SBA the IP addresses of the Consultant's systems from which remote testing will be conducted. Consultant assumes that if this address space is managed, wholly or in part, by a third-party vendor to the SBA, the SBA must notify the vendor of scheduled testing activities. Consultant will conduct application penetration testing against a single instance of each of the agreed upon applications in a single test environment.

General activities for this task to be performed by Consultant include:

- ◆ Step 1: Where available, review the SBA provided application vulnerability scan reports. Otherwise perform automated, unauthenticated scans of in-scope applications to generate application mapping and provide initial reporting of vulnerabilities.
- ◆ Step 2: Manually validate significant vulnerabilities reported by automated scans and attempt exploitation.
- ◆ Step 3: Perform manual testing of the in-scope applications to discover and exploit application logic-based vulnerabilities and other vulnerabilities difficult to discover via automated scans.

Consultant will conduct the following activities:

- ◆ Conduct information reconnaissance to assess information leakage, the potential to misuse the application to access the SBA information in an unintended way, and the opportunity to corrupt data stores through malicious data entry

♦ Test for OWASP Top 10 Web Application Security Risks such as:

- Injection attacks (SQL, NoSQL, OS, LDAP)
- Broken authentication / authentication bypass
- Sensitive data exposure
- XML External Entities
- Broken access controls / Circumvention of access controls
- Security misconfigurations
- Cross-site-scripting (XSS)
- Insecure deserialization
- Using components with known vulnerabilities
- Insufficient logging and monitoring

♦ Exploit any discovered vulnerabilities to:

- Attempt to gain access to system and user credentials
- Attempt to grant permissions to an unauthorized user
- Attempt to escalate user privileges
- Attempt to interact directly with backend database systems, via weaknesses in the application user interface
- Attempt to leverage discovered vulnerabilities, as applicable, to perform unauthorized actions
- Attempt to exploit vulnerabilities in scripts and java-based components
- Attempt to identify any sensitive information stored in system logs as applicable

♦ Monitor and conduct traffic analysis on the communications between client / web browser and backend servers (e.g. web servers, API servers, database, middleware and other supporting servers) as feasible.

- Attempt to conduct man-in-the-middle attacks via web application proxy tools
- Attempt to modify and manipulate messaging between systems
- Attempt to inject upstream messages to affect, alter or disrupt business operations systems and make unauthorized changes
- Attempt to inject downstream messages to affect, alter or disrupt systems and make unauthorized changes

♦ Attempt to extract system and user credentials

♦ Attempt to discover hidden and/or unused web services

Social Engineering: Consultant will apply a custom approach whereby the Consultant will test deceptions tailored to the SBA's business operation, including:

- ♦ Phishing/spear phishing/whaling
- ♦ Vishing/Phone-based social engineering
- ♦ Rogue Wi-Fi network access points

♦ Physical (tailgating, talk your way)

♦ Exploitable portable media

Physical Site Assessment: During customer site visits, Consultant conducts an external site assessment for physical security controls. Consultant observes the activities at the location, the movement of people and goods, the means to access the building, and the handling of deliveries and contractors. Consultant will ascertain whether procedures in use comply with SBA security policies. Consultant will try to gain unauthorized physical access to SBA facilities.

IV. Internal Network Assessments and Testing:

Consultant will conduct testing from an adversary perspective with VPN connectivity to the SBA's internal network.

Modeling an adversary, Consultant will try to gain internal network access, and discover and exploit weaknesses that lead to unauthorized computer access, with the goal of elevated privileges (e.g. Domain Admin credentials) or obtaining access to sensitive data.

This task focuses on validating the security controls that limit network access, including mechanisms to segment different security domains within the target infrastructure. Network security vulnerabilities will be identified from an active port, services and server platform perspective. Consultant penetration testers, using their penetration testing laptops will connect to SBA's internal network through a VPN end-point using SBA provided standard user accounts.

General activities for this task include:

♦ Step 1:

- **Review of Report on Vulnerable Operating System and Service Software Versions and Configurations:** Review SBA vulnerability reports for operating systems and service software that may be used by an attacker to retrieve sensitive system information or compromise the security of in-scope networks or systems.

♦ Step 2:

- **Vulnerable Communications between Servers:** Review network traffic flows to potentially identify insecure network communications between resources. Perform attacks that may disrupt normal system operations or inject traffic that may cause the system to operate in an unexpected way.

- **Exploitation of Vulnerabilities:** Conduct controlled and coordinated exploitation of reported vulnerabilities on select in-scope targets to compromise the host, obtain elevated privileges (e.g., root access, Domain Admin credentials), gain access to additional systems (pivot) or locate sensitive data, and attempt to move laterally within the infrastructure.

Consultant may conduct the following:

- ◆ Monitor network traffic using specialized hardware and software tools to identify network port utilization, encryption usage and protocol identification
- ◆ Manually validate vulnerabilities reported in provided scans report(s)
- ◆ Attempt to manually exploit validated vulnerabilities
- ◆ Attacks on the networks and computer systems may include, but are not limited to, the following:
 - ◆ IP/MAC Address Spoofing
 - ◆ Impersonation
 - ◆ Man-in-the-Middle Attacks
 - ◆ Monitoring/Eavesdropping
 - ◆ Traffic Redirection
 - ◆ Buffer Overflows
 - ◆ Exploitation of OS Weaknesses
 - ◆ Control of Management Interfaces
 - ◆ Firewall Evasion
 - ◆ Intrusion Detection System Evasion
 - ◆ Encryption downgrading
 - ◆ Post exploitation
 - Pivoting
 - Lateral Movement
 - System Password Cracking
 - Privilege Escalation
 - ◆ Virus Detection Evasion

Wireless 802.11x Infrastructure: Consultant will employ tools to enumerate and attempt unauthorized connections to existing Wi-Fi network access points as well as test for weak encryption and weak authentication associated with SBA's 802.11 technologies.

Approach to Grey Box Assessments: Consultant will define a grey box threat model with the SBA and perform testing following the model to assess threats against available ports and services on the server assets. To properly execute testing against the web application, Consultant uses both automated and manual techniques including viewing page source and manual fuzzing of various parameters in the Hypertext Transfer Protocol (HTTP) methods and cookies used by the application. Additionally, to execute testing against ports and services, our team uses open-source tools including Nmap, Ncat, and a wide variety of tools found in the Offensive Security Kali Penetration Testing image.

Assets within the testing scope can include but are not limited to financial systems, mission-sensitive systems, and general support system networks that collect, process, maintain, transmit, and record financial and/or mission-critical data. Those assets, which are determined to be SBA-owned but are hosted by third-party providers outside of the SBA may

be placed within scope; however, precautions must be taken to ensure no impact to the third-party provider and that testing does not violate Terms of Service (ToS).

Approach to Data Loss Prevention Assessments: With each Data Loss Assessment, Consultant will work with the SBA to define the in-scope configuration components and rules to be assessed. Consultant will then prepare to conduct the assessment. This includes preparing automated and manual tools to evaluate component configuration as well as identify, collect, and review the applicable rules and policies associated with the components in scope. Consultant will assess whether procedures in use comply with SBA security policies. Depending on the objectives of the assessment, Consultant may also plan, prepare, and execute data exfiltration tests to assess SBA controls.

Consultant will prepare a detailed report of the assessment approach, findings, and recommendations.

Third Party Risk Assessment: Additionally, in respect to data loss prevention, Consultant recognizes that the SBA's information and systems are part of a larger ecosystem that includes third parties. These third parties may interface with the SBA's systems, access the SBA's data, and store it within the third party's network, presenting cybersecurity risks to the SBA. Consultant will assist the SBA in evaluating the SBA's policy and technical controls as they relate to third parties.

The extent to which an evaluation may occur depends upon the SBA's agreements with the SBA's third parties. Consultant will review the following when evaluating how the SBA manages third party security.

- ◆ The data the third party must access
- ◆ The likelihood of unauthorized data disclosure, transmission errors or unacceptable periods of system unavailability caused by the third party
- ◆ Past performance between the parties
- ◆ Third Party/SBA security contract provisions
- ◆ Third party adoption of recognized industry standards, and accreditations
- ◆ The business impact if the risk event occurs (e.g., loss of money, breach of contract, loss of business opportunity, personal injury, statutory violation, reputational harm)

In evaluating the SBA's third-party security policy controls, Consultant will assess these controls from the principle of least privilege:

- ◆ What is the inherent risk of the activity performed by the third party?
- ◆ Would the activity be less risky if performed by the SBA?

- ◆ What security controls have been agreed upon with the SBA by the third party with respect to other globally accepted frameworks (e.g., ISO, COBIT)?
- ◆ Can these controls be cross-referenced within the NIST Cybersecurity Framework?

From this assessment, Consultant will be able to provide useful observations about the SBA's management of third-party security controls and provide recommendations to improve upon them.

In addition to policy control assessments, Consultant will be able to assess data exchanged with the third party to ensure what is being shared meets the SBA's policy and technical security controls.

Tools: Consultant uses a suite of commercial, open source and proprietary software and hardware tools to perform vulnerability assessments, penetration testing, and social engineering testing. This suite of tools is configured to minimize service impact, produce reliable and reproducible results, and identify critical risks while minimizing false positives. Consultant will not intentionally perform any testing that may cause service interruption, but all penetration and vulnerability testing is invasive, and fragile systems could be affected. Consultant will configure test tools to mitigate degradation of systems and networks, and will make no permanent changes to tested systems.

Consultant maintains its own penetration testing laptops, cybersecurity assessment toolkit, and software licenses for commercial vulnerability scanning and exploit software tools. Consultant's toolkit also includes its own custom developed vulnerability scanning and exploit software tools. Consultant's Vulnerability Assessment Toolkit is installed on Consultant-owned laptops, which are reimaged after each assessment.

V. Deliverables:

Status Reporting:

Consultant shall prepare weekly project status reports to be submitted to the SBA. The Consultant's Project Manager will work with the SBA Project Manager to define the standard content to be included in the report, which may include the following:

- ◆ Project Status Summary
- ◆ Schedule Status against the Project Plan
- ◆ Significant Issues and Actions to be taken by Consultant and/or the SBA
- ◆ Significant Decisions at prior status meeting
- ◆ Significant Risks and Actions to be taken by Consultant and/or the SBA

Assessment Report:

Consultant will document its findings, interpretation of risk and impact and recommendations resulting from the security assessment in a Deliverable Report to consist of the following sections.

- ◆ Executive Summary
- ◆ Findings Overview
- ◆ Scope and Methodology
- ◆ Test Environment
- ◆ Detailed Security Findings

Executive Summary provides the SBA a management level overview of the security assessment results with key findings, threats and risk, and strategic recommendations to improve the security posture of the SBA infrastructure.

Findings Overview provides one or more matrices or embedded spreadsheets to summarize the findings. Each finding will be listed with a:

Finding headline, descriptive title, its severity rating, the applicable security domain, the objective observation/measurement, and as deemed appropriate the impacted hardware, configuration and firmware version of the component to which the finding applies, and related recommendation. Where feasible it should include IP address, associated host name, and evidence. Findings should be numbered uniquely and consistently throughout the report for purposes of monitoring and follow-up in the next fiscal year.

Scope and Methodology defines the applications, network infrastructure, systems and components under assessment, the methodology and technical approach used by Consultant to perform the authorized assessment, and the risk assessment methodology to rate the findings.

Test Environment details the configuration of the environment used to conduct the testing, the product model, software version, hardware version and firmware of the components tested, and the test equipment and tools used by Consultant, as applicable.

Detailed Security Findings presents each finding, which will be assigned one of four severity levels based on the Consultant risk assessment model that uses a four-tier rating system where each security finding is assigned a severity rating:

- ◆ An Exposure (high risk) is a vulnerability, a security weakness with a proven or highly probable method of exploitation.
- ◆ A Concern (medium risk) is foremost a security weakness that either satisfies known threat objectives or can result in significant damage if successfully exploited, but not both.

◆ A Shortcoming (low risk) is a security weakness that does not satisfy known threat objectives and will not result in significant damage if successfully exploited.

◆ A Remark documents an item worthy of note.

Consultant rates risk based on the severity of the exploit as well as the potential impact to the SBA's applications, access to sensitive data, potential compromise of user security and/or risk to business continuity.

Findings are addressed in order of priority and each finding is presented in four (4) parts:

◆ CVSSv3 Score: Where deemed applicable Consultant will provide a NIST Common Vulnerability Scoring System version 3 (CVSSv3) score for the finding.

◆ Observation/Measurement: Consultant will summarize the objective and repeatable evidence for each security finding that was discovered, observed, measured or otherwise acquired by Consultant. This section will describe the step-by-step process to discover and replicate the findings supported by screenshots.

◆ Risk/Impact Discussion: Consultant will interpret the evidence for the finding, provides its opinion about what an adversary might accomplish by exploiting the finding, and renders an opinion about risk or impact that may result from a successful attack.

◆ Remediation Recommendation(s): Consultant will document its advice and corrective actions to mitigate the risk and remediate the security finding based on best practices and industry standards, with specific mitigations for all findings that present significant risk.

Consultant will provide a draft version of the Deliverable Report after completion of testing for the SBA to review and comment. Consultant will address the SBA comments and provide a final Deliverable Report. Consultant will provide all reports to the SBA in a secure electronic format.

Presentation to the SBA Audit Committee:

The SBA may elect to have a presentation of the findings made to the SBA Audit Committee so that Consultant can answer questions about the testing and its results. Consultant's Project Manager will work with the SBA Project Manager to define the agenda and content to be included in the presentation to the SBA Audit Committee.

Deliverable Quality Review Process:

Prior to submitting to the SBA, a deliverable (draft or final), Consultant will conduct an internal review, known as a Work Product Review (WPR). The process for Consultant's team to complete a deliverable with Consultant's quality review will follow these basic steps:

◆ Deliverable developed by team and submitted for WPR through Project Manager

- ◆ A deliverable review team, that includes the SBA's Security Lead and the Project Manager (may include others as needed depending on the deliverable) reviews the draft deliverable, and provides formal comments on the draft.
- ◆ The comments are reviewed by the team, and the deliverable is updated/modified accordingly.
- ◆ The modified deliverable is reviewed for incorporation of the WPR feedback by the Project Manager and approved for customer submission.
- ◆ The draft assessment report is provided to the SBA for an external review, feedback is reviewed and incorporated into the final Deliverable.
- ◆ The Deliverable is submitted to the SBA.

SCHEDULE B:

DATA SECURITY ADDENDUM AND SYSTEMS USE AGREEMENT

STATE BOARD OF ADMINISTRATION DATA SECURITY ADDENDUM

1 DATA SECURITY STANDARDS

Consultant shall comply with either the provisions of applicable SBA policies (SBA Policy #20-404 Remote Access; SBA Policy #20-411 Anti-Virus; and SBA Policy #10-409 Confidential/Sensitive Electronic Data Handling), as amended from time to time, or NIST SP 800 Series, ISO/IEC 27000 Series, or a comparable similar industry standard. Consultant will provide immediate notice to the SBA of any known or suspected violation of any SBA policy or industry standard.

2 NONDISCLOSURE

SBA Data shall be considered confidential and proprietary information to the extent permitted by Florida or other applicable law. Consultant shall hold SBA Data in confidence and shall not disclose SBA Data to any person or entity, whether internal or external to the Consultant, except those persons that are directly involved with performing the duties under the Agreement and that further have a need to know the SBA Data in order to carry out their duties under the Agreement. Additionally, SBA Data may be disclosed when the disclosure is authorized by the SBA or is specifically required by law. For purposes of this Section 2, Data Security, "SBA Data" means all data accessed, created, maintained, obtained, processed, stored, or transmitted by Consultant in the course of performing the Agreement and all information derived therefrom.

3 LOSS OR BREACH OF DATA

Consultant shall provide immediate notice to the SBA in the event it becomes aware of any security breach other than that occasioned by the Consultant in performing its services under the Agreement or any unauthorized transmission or loss of any SBA Data. In the event of loss or destruction of any SBA Data where such loss or destruction is due to the fault or negligence of Consultant, Consultant shall be responsible for recreating such lost or destroyed data in the manner and on the schedule set by the SBA, at Consultant's sole expense and in addition to any other damages the SBA may be entitled to by law or this Agreement. In the event lost or damaged data is suspected, Consultant will perform due diligence, report findings to the SBA, and take all reasonable measures necessary to recover the data. If such data is unrecoverable, Consultant will pay costs to remediate and correct the problems caused by or resulting from each loss or destruction of data (including the cost to notify third parties and to provide credit monitoring services to third parties), in addition to any other damages the SBA may be entitled to by law or this Agreement. Consultant acknowledges that failure to maintain security that results in a breach of data may subject this Agreement to the administrative sanctions for failure to comply with Section 501.171, Florida Statutes, together with liability for any costs to the SBA of such breach of security caused by Consultant.

For all claims against the Consultant, and, in the absence of negligence, willful misconduct, fraud or bad faith by the Consultant, Consultant's liability under the Agreement for direct damages shall be limited to the greater of \$100,000, the dollar amount of the fees paid under this Agreement, or the one-time charges rendered by Consultant under this Agreement. Neither party shall be liable to the other for special, indirect, punitive, or consequential damages, including lost data or records, even if the other party had been advised that such damages are possible. No party shall be liable for lost profits or lost revenue. In circumstances where all or any portion of the provisions of this paragraph are finally judicially determined to be unavailable, the aggregate liability of Consultant, its subcontractors and their respective personnel for any claim shall not exceed an amount that is proportional to the relative fault that Consultant's conduct bears to all other conduct giving rise to such claim.

The limitation on damages contained in this section or in the Agreement is enforceable only to the fullest extent permissible under Florida law.

4 SECURITY AUDITS

If SBA Data will reside in Consultant's system, the SBA may conduct, or may request Consultant to conduct at Consultant's expense, an annual network penetration test or security audit of Peraton's system(s) on which SBA Data resides. If the term of the Agreement is less than a year long, the penetration test or security audit of Consultant's system(s) on which SBA Data resides, may be exercised at any time during the term of the Agreement.

5 DATA PROTECTION

No SBA Data will be transmitted or shipped to entities outside of the United States of America, nor will it be stored or processed in systems located outside of the United States of America, regardless of the method or level of encryption employed. Access to SBA Data shall only be available to authorized Consultant Representatives that have a legitimate business need. For purposes of this Addendum, "Consultant Representatives" means Consultant's officers, directors, employees, agents, contractors, subcontractors and consultants (including affiliates thereof). Requests for access to the SBA's information technology resources shall be submitted to the SBA's Support and Office Services ("Help Desk") staff. With the SBA's approval, Consultant Representatives may be granted access to SBA information technology resources as necessary for fulfillment of related responsibilities. Prior to the provision of access to SBA information technology resources, Consultant agrees to provide the Consultant Representative a written copy of the SBA's Systems Use Agreement as attached below (which may be amended by the SBA from time to time in the SBA's sole discretion upon providing notice to Consultant (the "Systems Use Agreement"). At such time as the SBA provides access to SBA technology resources, Consultant and any Consultant Representative who has access to SBA technology resources will be deemed to have agreed to the Systems Use Agreement (as defined above). Further, Consultant agrees to be responsible in the event any Consultant Representatives breach any of the terms set forth in the Systems Use Agreement. Remote connections are subject to detailed monitoring as deemed appropriate by the SBA.

6 ENCRYPTION

Consultant shall encrypt all SBA Data, in transmission and at rest, using an SBA approved encryption technology.

7 BACK-UPS

Consultant shall maintain and secure adequate back-ups of all documentation and programs utilized to process or access SBA Data.

8 DATA SECURITY PROCEDURES

Consultant has established appropriate administrative, technical, and physical safeguards to protect the confidentiality of, and to prevent the unauthorized use or access to, SBA Data. Consultant shall have data security procedures to ensure only authorized access to data and databases by Consultant Representatives for purposes of performing the Agreement and to ensure no unauthorized access to data or databases by individuals or entities other than those authorized by the Agreement or the SBA. Consultant shall ensure that access to data and databases by Consultant Representatives will be provided on a need to know basis and will adhere to the principle of least privilege. (The principle of least privileged means giving a user account only those privileges which are essential to perform its intended function.)

9 OWNERSHIP OF DATA

Consultant shall provide to the SBA, upon its request, SBA Data in the form and format reasonably requested by the SBA. Consultant will not sell, assign, lease, or otherwise transfer any SBA Data to third parties, or commercially exploit SBA Data, except as authorized by the SBA. Consultant will not possess or assert any lien or other right against or to any SBA Data in any circumstances. SBA Data is and shall remain the exclusive property of the SBA. SBA Data created by Consultant, obtained by Consultant from a source other than the SBA, or derived from SBA Data will become property of the SBA immediately upon the creation, receipt or derivation of such data, as applicable.

10 BACKGROUND CHECKS

Consultant shall confirm that their representatives (which includes Consultant's officers, directors, employees, agents, contractors, subcontractors and consultants, including affiliates thereof) assisting in the performance of the Agreement have passed appropriate, industry standard, background screening (include criminal background checks) and possess the qualifications and training to comply with the terms of the Agreement, before being provided access to SBA Data. Upon the SBA's request, Consultant shall provide to the SBA an attestation that the foregoing background checks have been completed.

11 COMPLIANCE

Consultant represents and warrants that it is in compliance with, and agrees and covenants that it will at all times during the term of the Contract continue to be compliance with, all applicable laws, regulations and industry standards (including, without limitation, all applicable laws, regulations and industry standards relating to cybersecurity or data collection, storage, security or privacy).

12 RETURN/ DESTRUCTION OF SBA DATA

Consultant shall not at any time destroy any SBA Data it holds without the prior written consent of the SBA. If requested by the SBA, within 30 days of the completion, termination or expiration of the Agreement, Consultant will transfer SBA data to the SBA (if so directed by the Agreement), or, unless otherwise required by any applicable law (including, for the avoidance of doubt, Florida's record retention laws), destroy all SBA data possessed by Consultant. Consultant shall provide the SBA documentation affirming the completion of any SBA requested data transfer (including confirmation of receipt by the SBA) and the destruction of any SBA Data possessed by Consultant. Notwithstanding the foregoing, Consultant may, in accordance with applicable legal, disaster recovery and professional requirements, store copies of SBA Data in an archival format which may not be immediately returned or destroyed but which would remain subject to the confidentiality obligations set forth in the Agreement.

13 BUSINESS CONTINUITY PLAN/ DISASTER RECOVERY

Consultant has implemented and will maintain business continuity and disaster recovery plans designed to minimize interruptions of services and ensure recovery of systems and applications used to provide the services under this Agreement. Such plans cover the facilities, systems, data, applications and employees that are critical to the provision of the services, and will be tested at least annually to validate that the recovery strategies, requirements and protocols are viable and sustainable. Consultant shall provide an executive summary of such plans setting forth prioritized threats, time criticality of business functions, resources needed to successfully recover, employee training and communication, and potential costs of recovery, as well as, including an assessment of the plans' most recent test results, to the SBA upon request. In the event of a business disruption that materially impacts (or is reasonably expected to materially impact) Peraton's provision of services under this Agreement, Consultant will promptly notify the SBA of the disruption and the steps being taken in response.

IN WITNESS WHEREOF, each party has caused this Data Security Addendum to be executed by its respective duly authorized officer, as of June 13, 2022 (the "Effective Date").

SBA:
STATE BOARD OF ADMINISTRATION
OF FLORIDA

[Redacted Signature Block]

CIO

CONSULTANT:
PERATON STATE & LOCAL INC.

[Redacted Signature Block]

[Redacted Signature Block]

LEGAL COUNSEL

Systems Use Agreement

THE FOLLOWING ARE THE TERMS OF SYSTEMS USE DESCRIBED IN SECTION 5 ABOVE. THESE TERMS MUST BE PROVIDED TO USER PRIOR TO ACCESSING ANY SBA SYSTEM.

1.1 Ownership of Data

SBA Data is and shall remain the exclusive property of the SBA. User shall use SBA Data solely for authorized purposes. SBA Data created by User, obtained by User from a source other than the SBA, or derived from SBA Data will become property of the SBA immediately upon the creation, receipt or derivation of such data, as applicable. For purposes of this Systems Use Agreement, "SBA Data" means all information accessed, created, maintained, obtained, processed, stored, or transmitted using any SBA Account or SBA Systems and all information derived therefrom. "SBA Systems" means any of the following:

- a. Any desktop, laptop, server, or other information technology resource (whether physical or virtual) under the administration or ownership of the SBA, wherever located;
- b. All business applications, including any related data, system services and functions provided by or under the administration or ownership of the SBA. "User" means any Consultant Representative that will have access to information technology Systems of the State Board of Administration of Florida.

1.2 Nondisclosure

SBA Data shall be considered confidential and proprietary information to the extent permitted by Florida or other applicable law. User shall hold SBA Data in confidence and shall not disclose SBA Data to any person or entity except as authorized by the SBA or as required by law.

1.3 Privacy

User does not have a right to privacy regarding any activity conducted using the SBA Systems. The SBA can review, read, access or otherwise monitor all activities on the SBA Systems or on any other systems accessed by use of the SBA Systems, and purge any or all information on the SBA Systems. The use of a password does not create a right to privacy in the SBA Systems.

1.4 Credentials

Only persons who are authorized by the SBA may use SBA Systems. User shall not share SBA Account credentials with any other person, including but not limited to sharing of credentials with other authorized users. User shall immediately change User's password should it become known by any other person. For purposes of this Systems Use Agreement, "SBA Account" means any set of system access credentials (e.g., a user ID and password) provided by the SBA.

1.5 Copyright

User shall not make copies of applications running on SBA Systems for use at home, on laptops, or for any other reason, without SBA authorization. User shall not import, download, copy or store SBA Data (including without limitation, emails) onto non-SBA owned devices without SBA authorization. User shall not import, download, copy, or store copyrighted material without permission from the copyright owner.

1.6 Anti-virus

If User accesses the SBA network remotely, User shall do so only on devices with industry standard, supported anti-virus software installed. This software must be active, be scheduled to perform virus checks at regular intervals, and have its virus definition files kept up to date.

1.7 Installation

User shall not install any applications, programs, applets, or snap-ins on any SBA equipment.

1.8 Authorized access

User shall not access (or attempt to gain access to) any SBA Account or SBA System other than that to which the User is authorized.

1.9 Authorized Use

User shall not use any SBA Account or SBA System to transmit, distribute, or store content or materials in a manner that violates SBA policies, U.S. state and federal laws, the laws of jurisdictions outside of the U.S., or the Systems Use Agreement.

1.10 Data Security Standards

User shall comply with either the provisions of applicable SBA policies (SBA Policy #20-404 Remote Access; SBA Policy #20-411 Anti-Virus; and SBA Policy #10-409 Confidential/Sensitive Electronic Data Handling), as amended from time to time, or NIST SP 800 Series, ISO/IEC 27000 Series, or a comparable similar industry standard. User will provide immediate notice to the SBA of any known or suspected violation of any SBA policy or industry standard.

1.11 Violation Reporting

If User becomes aware of (or suspects there may have been) any violation of the Systems Use Agreement, User shall contact the SBA Support and Office Services ("Help Desk") at 850-413-1100 to report the situation.

1.12 Violation Penalties

User understands the Systems Use Agreement. User understands that violation of the Systems Use Agreement may lead to penalties imposed by U.S. state and federal laws, and/or the laws of jurisdictions outside of the U.S.

1.13 Indemnification

User agrees to protect, indemnify, defend and hold harmless the SBA, its trustees, officers and employees from and against any and all costs, claims, demands, damages, losses, liabilities and expenses (including reasonable counsel fees and expenses, and investigation, collection, settlement and litigation costs) resulting or arising from or in any way related to User's breach of data security, negligent acts or omissions, fraud, willful misconduct, violation of law, or breach of the Systems Use Agreement.

1.14 Public Records Compliance

User acknowledges that SBA Data will constitute "public records" which will be subject to public access and disclosure under Chapter 119, Florida Statutes unless such records are exempt from disclosure under Chapter 119, Florida Statutes. To the extent applicable, User shall comply with Chapter 119, Florida Statutes. In particular, User shall:

- a. Keep and maintain public records required by the SBA in order to perform the services under any applicable contract for services with the SBA ("Contract");
- b. Upon request from the SBA's custodian of public records, provide the SBA with a copy of the requested records or allow the records to be inspected or copied within a reasonable time at a cost that does not exceed the cost provided in Chapter 119, Florida Statutes or as otherwise provided by Florida law;
- c. Ensure that public records that are exempt or confidential and exempt from public records disclosure requirements are not disclosed except as authorized by law for the duration of the term of the Contract and following completion of the Contract if User does not transfer the records to the SBA; and
- d. Upon completion of the Contract, transfer, at no cost, to the SBA all public records in User's possession (if so directed by the SBA) or keep and maintain public records required by the SBA to perform the service. If User transfers all public records to the SBA upon completion of the Contract, User shall destroy any duplicate public records that are exempt or confidential and exempt from public records disclosure requirements. If User keeps and maintains public records upon completion of the Contract, User shall meet all applicable requirements for retaining public records. User shall provide all records that are stored electronically to the SBA, upon request from the SBA's custodian of public records, in a format that is compatible with the information technology systems of the SBA.

IF USER HAS QUESTIONS REGARDING THE APPLICATION OF CHAPTER 119, FLORIDA STATUTES, TO USER'S DUTY TO PROVIDE PUBLIC RECORDS RELATING TO THIS CONTRACT, CONTACT THE CUSTODIAN OF THE PUBLIC RECORDS AT:

**STATE BOARD OF ADMINISTRATION OF FLORIDA
POST OFFICE BOX 13300
TALLAHASSEE, FLORIDA 32317-3300
(850) 488-4406
SBAContracts_DL@SBAFLA.COM**

1.15 Governing Law; Venue

The Systems Use Agreement shall be construed and enforced in accordance with the laws of the State of Florida without regard to conflict of law principles. Any proceeding to resolve disputes regarding or arising out of the Systems Use Agreement shall be conducted in the state courts located in Leon County, Florida, and User hereby consents to the jurisdiction and venue of those courts.

1.16 Entire Agreement

THE SYSTEMS USE AGREEMENT AND ANY AND ALL EXHIBITS, SCHEDULES AND ENCLOSURES ATTACHED HERETO, WHICH ARE INCORPORATED INTO THE AGREEMENT BY THIS REFERENCE, CONSTITUTE AND EMBODY THE ENTIRE AGREEMENT AND UNDERSTANDING OF USER AND THE SBA WITH RESPECT TO THE SUBJECT MATTER HEREOF, SUPERSEDE ANY PRIOR OR CONTEMPORANEOUS AGREEMENTS OR UNDERSTANDINGS WITH RESPECT TO THE SUBJECT MATTER HEREOF, AND, UNLESS OTHERWISE PROVIDED HEREIN, CANNOT BE ALTERED, AMENDED, SUPPLEMENTED, OR ABRIDGED OR ANY PROVISIONS WAIVED EXCEPT BY WRITTEN AGREEMENT OF USER AND THE SBA.

IN WITNESS WHEREOF, the undersigned "User" hereby agrees to the provisions of this Agreement, as of the Effective Date set forth below.

USER:

Printed Name

Signature

Effective Date

Attachments: SBA Policy #10-400 Acceptable Use, SBA Policy #10-410 Passwords, SBA Policy #10-422 Email Communications/Internet Access Policy, SBA Policy # 20-404 Remote Access and SBA Policy #20-411 Anti-Virus