REQUEST FOR LEGAL SERVICES

To: County Attorney's Office
Attention: Sandra Howard

From: Sean Jones, Drawer No. AS04

Dept: Information Technology Ext.- 7608

Date: 06/13/2024

Emailed Jessica on 6/18/24 w/ comments. —SH

Request (in detail):

Requesting review of the Grant Agreement for State of Florida Local Government Cybersecurity Grant Program. This agreement covers the capabilities awarded to the county through the grant program, and represents a renewal of previously awarded capabilities, with no additional capabilities awarded. The awarded capabilities are currently in place and operational in the Polk County BoCC environment.

Time Limit: As soon as possible (due date Thursday, June 27, 2024)

- Entity name must be changed to "Polk County" or "Polk County, a political subdivision of the State of Florida" (NO BOCC)
- If $ value > $100k, must be approved by BOCC.

Please indicate any time limits involved and attach all necessary documentation.

For County Attorney office use only:
Assign to: Sandi Date: 6/14/24

County Attorney Project No.: 24-330
Logged out: 6/18/24 SH

Agenda Template for County Manager Signature

SUBJECT:

Grant Agreement for State of Florida Local Government Cybersecurity Grant Program

Pursuant to FL Statute §.0725, this information is exempt from public meetings and public records requirements

DESCRIPTION:

This agreement covers the capabilities awarded to the county through the grant program, and represents a renewal of previously awarded capabilities, with no additional capabilities awarded this year. The awarded capabilities are currently in place and operational in the Polk County BoCC environment, and are essential to securing the county's network environment.

RECOMMENDATION:

Recommendation is for the County Manager to approve and sign the Grant Agreement.

FISCAL IMPACT:

No fiscal impact.

CONTACT INFORMATIOIN:

Name: Sean Jones

Title: Cyber Security Analyst

Division: Information Technology

Phone: (863)534-7608

E-Mail: seanjones@polk-county.net

CHECKLIST:

Purple Sheet and Review – Legal	✓ SH 6/18/24
Division Fiscal Review	
Risk Review (if appropriate)	
Appropriate Insurance	
Deputy County Manager is Aware and Agrees	
Vendor Signature	

Comments/Notes:

Division Director Signature: _____ Date: 6/24/24

GRANT AGREEMENT

FOR

LOCAL GOVERNMENT CYBERSECURITY GRANT PROGRAM

CONTRACT NO: DMS-24/25-145

CATALOG OF STATE FINANCIAL ASSISTANCE NUMBER: 72.016

BETWEEN

THE STATE OF FLORIDA

DEPARTMENT OF MANAGEMENT SERVICES

AND

POLK COUNTY

Attn: James Loughlin
Information Security Officer
Polk County Board of County Commissioners
330 W. Church St.
Bartow, FL 33830

May 10, 2024

Congratulations Polk County Board of County Commissioners!

Your application for the Florida Local Government Cybersecurity Grant administered by the Florida Digital Service has been awarded. Based on the requests and information included in your application, the following capabilities will be offered:

Capability	Awarded Round 1	Solution	Quantity	Unit
External-Facing Asset Discovery	No	N/A	N/A	N/A
Endpoint-Based Asset Discovery (Agent)	No	N/A	N/A	N/A
Network-Based Asset Discovery (Agentless)	Yes	Armis	Large (Over 2501 FTE)	User Base
Content Delivery Network	No	N/A	N/A	N/A
Endpoint Detection & Response (EDR)	Yes	CrowdStrike	2500	Endpoints
Security Operations Platform	Yes	Reliaquest GreyMatter	Large	(1501-5000 FTE)
Email Security	Yes	Proofpoint	3000	Mailboxes

In addition to software access for the capabilities awarded, the Florida Digital Service will provide the following:

- Incident response assistance when requested.
- Training, technical assistance, and support for the capabilities granted.

The Department of Management Services will email you the Grant Agreement via DocuSign by Monday, May 13. To accept the capabilities being offered, we need your help to execute the Grant Agreement by June 27, 2024. If you identify any discrepancies with the information above, please contact us immediately.

The Florida Digital Service remains committed to supporting you throughout this process as we deploy critical capabilities to mitigate cybersecurity threats to your local community. We look forward to working alongside you and your team.

Regards,
Florida's Local Government Cybersecurity Grant Team
FL[Digital Service]
Cybersecuritygrants@digital.fl.gov

GRANT AGREEMENT

This Grant Agreement is made and entered into by and between the Department of Management Services (Department), an agency of the State of Florida (State), and Polk County (Grantee). The Department and the Grantee are sometimes referred to herein individually as a "Party" or collectively as the "Parties."

THIS AGREEMENT IS ENTERED INTO BASED ON THE FOLLOWING REPRESENTATIONS:

WHEREAS, the Department, through the Florida Digital Service (FL[DS]), has the authority, pursuant to Section 200, Fiscal Year 2024-2025 General Appropriations Act (GAA), to provide nonrecurring assistance to local governments for the development and enhancement of cybersecurity risk management programs; and

WHEREAS, the Grantee represents that it is fully qualified and eligible to receive the grant identified herein in accordance with the terms and conditions hereinafter set forth.

NOW THEREFORE, the Parties do mutually agree as follows:

A. Deliverables and Performance Requirements:

In accordance with the GAA, the Parties agree that the funds will be utilized as described in Attachment A – Solution Statement of Work. The Grantee shall provide the deliverables specified herein in accordance with the terms and conditions of this Agreement, including its attachments and exhibits.

B. Agreement Period:

The performance period for this Agreement begins upon execution and ends upon the expiration of the applicable cybersecurity technical assistance services or commodities awarded or purchased pursuant to the Agreement, or in accordance with the final implementation plan(s), unless terminated earlier in accordance with the Agreement. No renewals or extensions of this Agreement are permitted.

C. Agreement Documents and Amendments Thereto.

1. Agreement Documents. "Agreement" means this Grant Agreement and all incorporated attachments, exhibits, and schedules, which set forth the entire understanding of the Parties. There are no other provisions, terms, conditions, or obligations. This Agreement supersedes all previous oral or written communications, representations, or agreements on this subject.

   All attachments, exhibits, and schedules listed below are incorporated in their entirety into, and will form part of, this Agreement. In the event of a conflict, the following order of precedence shall apply:

   a. This Grant Agreement
   b. Attachment A – Solution Statement of Work
   c. Attachment B – Audit Requirements for Awards of State and Federal Financial Assistance, including its Exhibit 1
   d. Attachment C – Grantee Data Sharing Agreement(s) ("DSA"), if applicable

e. Final Implementation Plan, if applicable(s)

2. Counterparts. This Agreement may be executed in any number of counterparts, all of which taken together shall constitute one (1) single agreement between the Parties.

3. Survivability. This Agreement and any and all promises, covenants, and representations made herein are binding upon the Parties hereto and any and all respective heirs, assigns, and successors in interest. The respective obligations of the Parties, which by their nature would continue beyond the termination or expiration of this Agreement, including without limitation, the obligations regarding confidentiality, proprietary interests, and public records, shall survive termination or expiration of this Agreement.

4. Severability. If a court of competent jurisdiction deems any term or condition of this Agreement void or unenforceable, the other provisions are severable to that void provision, and will remain in full force and effect. However, to the fullest extent permitted by law, this Agreement shall be construed as if the scope or duration of such provision had been more narrowly drafted so as not to be invalid or unenforceable.

5. Amendments. With the exception of changes to the Primary Contacts, DSA/IT Coordinators, and the provisions of the applicable vendor terms and conditions, this Agreement may only be modified or amended by a written agreement duly executed by the Parties.

D. Notices and Primary Contacts:

1. Notices. The Parties shall use the contact information provided in Section D.2., Primary Contacts, below, for all communications and notices under this Agreement. Where the term "written notice" is used to specify a notice requirement herein, said notice will be deemed to have been given (i) when personally delivered; (ii) when transmitted via facsimile (with confirmation of receipt) or email (with confirmation of receipt), provided the sender on the same day sends a confirming copy of such notice by a recognized delivery service (charges prepaid); (iii) the Business Day immediately following the next Business Day on which the notice or communication has been provided prepaid by the sender to a recognized overnight delivery service; or (iv) on the date actually received except where there is a date of the certification of receipt. For purposes of this Agreement, "Business Day" means any day of the week, excluding weekends and holidays, observed by State agencies pursuant to section 110.117(1)(a)-(j), Florida Statutes (F.S.).

2. Primary Contacts.

a. **Department's Grant Manager** (see section 215.971, F.S.).

Lacy Perkins, Procurement & Grants Administrator
Florida Digital Service
Department of Management Services
2555 Shumard Oaks Blvd
Tallahassee, Florida 32399

Telephone: (850) 413-0604
Email: CybersecurityGrants@digital.fl.gov

2. **Grantee's Grant Manager**

James Loughlin, Information Security Officer
Polk County
330 W. Church St.
Bartow, Florida 33830
Telephone: +1 (863) 534-7564
Email: jamesloughlin@polk-county.net

3. Changes in Primary Contacts. Either Party may provide notice to the other Party by email identifying a change of a designated primary contact and providing the new contact information for the newly designated primary contact. Such notices must be sent to the other Party's Grant Manager and is sufficient to effectuate this change without requiring a written amendment to this Agreement.

E. Payment, Funding, and Award Considerations:

1. Fiscal Year. The funds utilized for this Agreement are from the State's 2024-2025 Fiscal Year, which begins July 1, 2024, and expires on June 30, 2025.

2. Services, Licenses or Commodities Awards. The Grantee agrees to implement services, licenses, or commodities described in Attachment A – Solution Statement of Work, according to the Final Implementation Plan(s), if applicable. All uses of the items described in Attachment A – Solution Statement of Work are subject to the terms and conditions of the DSA and applicable riders attached thereto.

3. Procurement. The Department agrees to purchase all commodities or services awarded to the Grantee on behalf of the Grantee as described in Attachment A – Solution Statement of Work.

F. Compliance with Law:

1. Applicable Law. The Parties shall comply with the applicable state and federal laws, rules, regulations, and policies, including, but not limited to, those identified in this Agreement.

2. Governing Law. The Grantee agrees that this Agreement is entered into in the State of Florida, and shall be construed, performed, and enforced in all respects in accordance with the laws, rules, and regulations of the State. Each Party shall perform its obligations herein in accordance with the terms and conditions of this Agreement. Without limiting the provisions of Section P, Dispute Resolution, the exclusive venue of any legal or equitable action that arises out of or relates to this Agreement shall be the appropriate State court in Leon County, Florida; in any such action, the Parties waive any right to jury trial. Except as otherwise

provided by law, the Parties agree to be responsible for their own attorney fees incurred in connection with disputes arising under the terms of this Agreement.

3. Ethics. The Grantee shall comply with the requirements of sections 11.062 and 216.347, F.S. The Grantee shall not, in connection with this or any other agreement with the State, directly or indirectly:

   a. Offer, confer, or agree to confer any pecuniary benefit on anyone as consideration for any State officer or employee's decision, opinion, recommendation, vote, other exercise of discretion, or violation of a known legal duty; or
   b. Offer, give, or agree to give to anyone any gratuity for the benefit of, or at the direction or request of, any State officer or employee. For purposes of this subsection b, "gratuity" means any payment of more than nominal monetary value in the form of cash, travel, entertainment, gifts, meals, lodging, loans, subscriptions, advances, deposits of money, services, employment, or contracts of any kind.

   Upon request of the Department's Inspector General, or other authorized State official, the Grantee shall provide any type of information the Inspector General deems relevant to the Grantee's integrity or responsibility. Such information may include, but shall not be limited to, the Grantee's business or financial records, documents, or files of any type or form that refer to or relate to this Agreement. The Grantee shall retain such records in accordance with the record retention requirements of Part V of Attachment B, Audit Requirements for Awards of State and Federal Financial Assistance.

4. Advertising. Subject to Chapter 119, F.S., the Grantee shall not publicly disseminate any information concerning this Agreement under any promotional activity, such as advertisements or press releases, without prior written approval from the Department.

5. Conflict of Interest. This Agreement is subject to Chapter 112, F.S. The Grantee shall disclose the name of any officer, director, employee, or other agent who has or potentially has a conflict of interest relating to this Agreement or funds received hereunder.

6. Records Retention. The Grantee shall retain all records made or received in conjunction with this Agreement for the longer of five (5) years after the end of this Agreement period and all pending matters or the period required by the General Records Schedules maintained by the Florida Department of State (available at: https://dos.myflorida.com/media/703328/gs1-sl-2020.pdf). If the Grantee's record retention requirements terminate prior to the requirements stated herein, the Grantee may meet the Department's record retention requirements for this Agreement by transferring its records to the Department at that time, and by destroying duplicate records in accordance with section 501.171, F.S., and, if applicable, section 119.0701, F.S. The Grantee shall adhere to established information destruction standards such as those established by the National Institute of Standards and Technology Special Publication 800-88, "Guidelines for Media Sanitization" (2014). See https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf.

G. Recoupment of Funds:

1. Notwithstanding the damages limitations of Section R, Limitation of Liability, if the Grantee's non-compliance with any provision of this Agreement results in additional costs or monetary loss to the Department or the State, the Department can recoup the costs or losses from monies owed to the Grantee under this Agreement or any other agreement between the Grantee and any State entity. In the event that the discovery of additional costs or losses arises when no monies are available under this Agreement or any other agreement between the Grantee and any State entity, the Grantee shall repay such costs or losses to the Department in full within thirty (30) days from the date of discovery or notification, unless the Department agrees, in writing, to an alternative timeframe. The Department shall not be liable for any penalties or costs associated with the Grantee's misuse of any purchases made pursuant to this Agreement.

2. If the Grantee or its independent auditor discovers that an overpayment has been made, the Grantee shall repay said overpayment within forty (40) calendar days without prior notification from the Department. In the event that the Department first discovers an overpayment has been made, the Department will notify the Grantee in writing. Should repayment not be made in a timely manner, the Department shall be entitled to charge interest at the lawful rate of interest on the outstanding balance beginning forty (40) calendar days after the date of notification or discovery. Refunds should be sent to the Department's Agreement Manager and made payable to the "Department of Management Services." If this Agreement is terminated for cause, the Department, at its discretion, may require that the Grantee return to the Department any funds that were used for purposes that are considered ineligible under this Agreement.

H. Audits and Records:

1. Representatives of the Department, the State's Chief Financial Officer, the State's Auditor General, and representatives of the federal government, shall have access to any of the Grantee's books, documents, papers, and records, including electronic storage media, as they may relate to this Agreement, for the purposes of conducting audits or examinations or making excerpts or transcriptions.

2. The Grantee shall maintain books, records, and documents in accordance with the generally accepted accounting principles to sufficiently and properly reflect all purchases made under this Agreement.

   The Grantee shall comply with all applicable requirements of section 215.97, F.S., and Attachment B, Audit Requirements for Awards of State and Federal Financial Assistance. If the Grantee is required to undergo an audit, the Grantee shall disclose all related party transactions to the auditor.

3. The Grantee shall retain all its records, financial records, supporting documents, statistical records, and any other documents, including electronic storage media, pertinent to this

Agreement in accordance with the record retention requirements of Part V of Attachment B, Audit Requirements for Awards of State and Federal Financial Assistance. The Grantee shall cooperate with the Department to facilitate the duplication and transfer of such records or documents upon the Department's request.

4. If awarded services, licenses, or commodities described in Attachment A – Solution Statement of Work, the Grantee shall include records of the start and end dates for all tasks in the Final Implementation Plan(s), if applicable. Additional requirements may be incorporated in the Final Implementation Plan(s).

5. The Grantee shall include the aforementioned audit and recordkeeping requirements in all approved subrecipient contracts and assignments.

I. Public Records and Records Production:

1. Identification and Protection of Confidential Information. Article 1, section 24, Florida Constitution, guarantees every person access to all public records, and section 119.011, F.S., provides a broad definition of "public record." As such, records submitted to the Department (or any other State agency) are public records and are subject to disclosure unless exempt from disclosure by law. The following records for agencies, as "agency" is defined in section 119.011(2), F.S., are confidential and exempt pursuant to section 119.0725, F.S.:

   a. Cybersecurity insurance limits and deductibles;
   b. Information relating to critical infrastructure;
   c. Incident reporting information pursuant to sections 282.318 and 282.3185, F.S.;
   d. Network schematics;
   e. Hardware and software configurations; and
   f. Encryption information or information that identifies detection, investigation, or response practices for suspected or confirmed cybersecurity incidents, including suspected or confirmed breaches.

   If the Grantee considers any portion of other records it provides to the Department (or any other State agency) to be trade secret or otherwise confidential or exempt from disclosure under Florida or federal law, the Grantee shall mark the document as "confidential" and simultaneously provide the Department (or other State agency) with a separate, redacted copy of the record. Such records and those records made confidential and exempt pursuant to section 119.0725, F.S., shall be considered "Confidential Information." For each portion redacted, the Grantee shall describe in writing the grounds for claiming the exemption, including the specific statutory citation for such exemption. The Grantee shall only redact portions of records that it claims are Confidential Information.

   In the event of a request for public records pursuant to Chapter 119, F.S., the Florida Constitution, or other authority, to which records that are marked as "confidential" are responsive, the Department will provide the Grantee-redacted copy to the requestor. If a requestor asserts a right to the redacted Confidential Information, the Department will notify

the Grantee such an assertion has been made. It is the Grantee's responsibility to take the appropriate legal action to assert that the information in question is exempt from disclosure under Chapter 119, F.S., or other applicable law.

If the Department becomes subject to a demand for discovery or disclosure of documents that are marked as "confidential" in a legal proceeding, the Department will give the Grantee notice of the demand or request. The Grantee shall take the appropriate legal action in response to the demand and to defend its claims of confidentiality. If the Grantee fails to take appropriate and timely action to protect the records it has designated as Confidential Information, the Grantee agrees that the Department is permitted to treat those records as not confidential and the Department is permitted to provide the unredacted records to the requester and the Grantee agrees not to pursue any suit, action, or claim, including for damages, against the Department or its employees, attorneys, agents or volunteers.

The Grantee shall protect, defend, and indemnify the Department from all suits, claims, actions, demands, liability, costs, fines, and attorneys' fees arising from or relating to the Grantee's determination that the redacted portions of its records are Confidential Information, including all costs, including attorney's fees, incurred regarding the entitlement or amount of such attorney's fees. If the Grantee fails to submit a redacted copy in accordance with this section, of information it claims is Confidential Information, the Department is authorized to produce the entire record submitted to the Department, including those records marked "confidential," in response to a public records request for, or demand for discovery or disclosure of, these records and the Grantee agrees not to pursue any suit, action, or claim, including for damages, against the Department or its employees, attorneys, agents, or volunteers.

2. Inspection of Records. In accordance with section 216.1366, F.S., the Department is authorized to inspect the: (a) financial records, papers, and documents of the Grantee that are directly related to the performance of this Agreement or the expenditure of State funds; and (b) programmatic records, papers, and documents of the Grantee which the Department determines are necessary to monitor the performance of this Agreement or to ensure that the terms of this Agreement are being met. The Grantee shall provide such records, papers, and documents requested by the Department within ten (10) Business Days after the request is made.

J. Non-Discrimination:

The Grantee shall not unlawfully discriminate against any individual employed in the performance of this Agreement due to race, religion, color, sex, physical handicap unrelated to such person's ability to engage in this work, national origin, ancestry, or age. The Grantee shall provide a harassment-free workplace, and any allegation of harassment shall be given priority attention and action.

K. Duty of Continuing Disclosure of Legal Proceedings and Instances of Fraud:

1. The Grantee shall provide written notice to the Department disclosing any criminal litigation, investigation, or proceeding that arises during the Agreement period involving the Grantee except where the Grantee is involved in a prosecutorial or administrative capacity, or, to the extent the Grantee is aware, any of the Grantee's subrecipients or contractors (or any of the foregoing entities' current officers or directors). The Grantee shall also provide written notice to the Department disclosing any civil litigation, arbitration, or proceeding that arises during the Agreement period that is related to or involves funds provided under this Agreement, to which the Grantee (or, to the extent the Grantee is aware, any subrecipient or contractor hereunder) is a party, and which:

    a. Might reasonably be expected to adversely affect the viability or financial stability of the Grantee or any subrecipient or contractor hereunder; or
    b. Involves a claim or written allegation of fraud against the Grantee, or any subrecipient or contractor hereunder, by a governmental or public entity arising out of business dealings with governmental or public entities.

    All notices under this section must be provided to the Department within thirty (30) Business Days following the date that the Grantee first becomes aware of any such litigation, investigation, arbitration, or other proceeding (collectively, a "Proceeding"). Details of settlements that are prevented from disclosure by the terms of the settlement must be annotated as such.

2. This duty of disclosure applies to each officer and director of the Grantee, subrecipients, or contractors when any Proceeding relates to the officer's or director's business or financial activities.

3. Instances of Grantee operational fraud or criminal activities, regardless of whether a legal Proceeding has been initiated, shall be reported to the Department's Grant Manager within twenty-four (24) hours of the Grantee being made aware of the incident.

4. The Grantee shall promptly notify the Department's Grant Manager of any Proceeding relating to or affecting the Grantee's, subrecipient's, or contractor's business. If the existence of such Proceeding causes the State to conclude that the Grantee's ability or willingness to perform this Agreement is jeopardized, the Grantee shall be required to provide the Department's Grant Manager all reasonable assurances requested by the Department to demonstrate that:

    a. The Grantee will be able to perform this Agreement in accordance with its terms and conditions; and
    b. The Grantee and/or its employees, agents, subrecipients, or contractor(s) have not and will not engage in conduct in performance under this Agreement that is similar in nature to the conduct alleged in such Proceeding.

L. Assignments, Subgrants, and Contracts:

1. Unless otherwise specified in Attachment A – Solution Statement of Work, or through prior written approval of the Department, the Grantee may not: 1) subgrant any funds awarded under this Agreement; 2) contract its duties or responsibilities under this Agreement out to a third party; or 3) assign, transfer, or sell any of the Grantee's rights or responsibilities, unless specifically permitted by law to do so. Any such subgrant, contract, or assignment occurring without the prior approval of the Department shall be null and void. In the event the Department approves transfer of the Grantee's obligations, the Grantee remains responsible for all work performed and all expenses incurred in connection with this Agreement. In addition, this Agreement shall bind the successors, assigns, and legal representatives of the Grantee, and of any legal entity that succeeds the Grantee, to the Grantee's obligations to the Department.

2. The Grantee agrees to be responsible for all work performed in fulfilling the obligations of this Agreement.

3. The Grantee agrees that the Department may assign or transfer its rights, duties, or obligations under this Agreement to another governmental entity upon giving prior written notice to the Grantee.

M. Intellectual Property Rights:

Where activities supported by this Agreement result in the creation of intellectual property rights, the Grantee shall notify the Department, and the Department will determine whether the Grantee will be required to grant the Department a perpetual, irrevocable, royalty-free, nonexclusive license to use, and to authorize others to use for State government purposes, any resulting patented, copyrighted, or trademarked work products developed under this Agreement.

N. Independent Contractor Status:

It is mutually understood and agreed to that at all times during the Grantee's performance of its duties and responsibilities under this Agreement that Grantee is acting and performing as an independent contractor. The Department shall neither have nor exercise any control or direction over the methods by which the Grantee shall perform its work and functions other than as provided herein. Nothing in this Agreement is intended to or shall be deemed to constitute a partnership or joint venture between the Parties.

1. The Grantee (and its officers, agents, employees, subrecipients, contractors, or assignees), in performance of this Agreement, shall act in the capacity of an independent contractor and not as an officer, employee, or agent of the State. Further, unless specifically authorized to do so, the Grantee shall not represent to others that, as the Grantee, it has the authority to bind the Department or the State.

2. Neither the Grantee nor its officers, agents, employees, subrecipients, contractors, or assignees, are entitled to State retirement or State leave benefits, or to any other compensation of State employment as a result of performing the duties and obligations of this Agreement.

3. The Grantee agrees to take such actions as may be necessary to ensure that each subrecipient or contractor will also be deemed to be an independent contractor and will not be considered or permitted to be an agent, servant, joint venturer, or partner of the State.

4. Unless agreed to by the Department in Attachment A – Solution Statement of Work, the Department will not furnish services of support (e.g., office space, office supplies, telephone service, secretarial, clerical support, etc.) to the Grantee or its subrecipient, contractor, or assignee.

5. The Department shall not be responsible for withholding taxes with respect to the Grantee's compensation hereunder. The Grantee shall have no claim against the Department for vacation pay, sick leave, retirement benefits, social security, workers' compensation, health or disability benefits, reemployment assistance benefits, or employee benefits of any kind. The Grantee shall ensure that its employees, subrecipients, contractors, and other agents, receive benefits and necessary insurance (health, workers' compensation, reemployment assistance benefits) from an employer other than the State.

6. At all times during the Agreement period, the Grantee must comply with the reporting and Reemployment Assistance contribution payment requirements of chapter 443, F.S.

O. Termination:

1. Termination for Failure to Implement. For awarded services, licenses, or commodities under Attachment A – Solution Statement of Work, if the Grantee does not approve a Final Implementation Plan within 15 calendar days of purchase order issuance for the awarded solutions, this Agreement may be terminated by the Department, at its sole discretion.

2. Termination Due to the Lack of Funds. The funds utilized for this Agreement are from the State's 2024-2025 Fiscal Year, which begins July 1, 2024, and expires on June 30, 2025. If funds become unavailable for this Agreement's purpose, such event will not constitute a default by the Department or the State. The Department agrees to notify the Grantee in writing at the earliest possible time if funds are no longer available. In the event that any State funds upon which this Agreement depends are withdrawn or redirected, the Department may terminate this Agreement by providing written notice to the Grantee. The Department will be the final authority as to the availability of funds.

3. Termination for Cause. The Department may terminate this Agreement if the Grantee fails to:

   a. Satisfactorily complete the deliverables within the time specified in this Agreement;
   b. Maintain adequate progress, thus endangering performance of this Agreement;
   c. Honor any term of this Agreement; or

d. Abide by any statutory, regulatory, or licensing requirement.

The Grantee shall continue to perform any work not terminated. The Department's rights and remedies in this clause are in addition to any other rights and remedies provided by law or under this Agreement. The Grantee shall not be entitled to recover any cancellation charges or lost profits.

4. Termination for Convenience. The Department may terminate this Agreement, in whole or in part, by providing written notice to the Grantee that the Department determined, in its sole discretion, it is in the State's interest to do so. The Grantee shall not furnish any product or continue services after the specified termination date in the Department's notice of termination, except as necessary to complete the continued portion of this Agreement, if any. The Grantee will not be entitled to recover any cancellation charges or lost profits.

5. Grantee's Responsibilities upon Termination. If the Department provides a notice of termination to the Grantee, except as otherwise specified by the Department in that notice, the Grantee shall:

   a. Stop work under this Agreement on the date and to the extent specified in the notice.
   b. Complete performance of such part of the work that has not been terminated by the Department, if any.
   c. Take such action as may be necessary, or as the Department may specify, to protect and preserve any property which is in the possession and custody of the Grantee, and in which the Department has or may acquire an interest.
   d. Transfer, assign, and make available to the Department all property and materials belonging to the Department upon the effective date of termination of this Agreement. No extra compensation will be paid to the Grantee for its services in connection with such transfer or assignment.

P. Dispute Resolution:

Disputes concerning performance under this Agreement will be decided by the Department, who shall reduce the decision to writing and serve a copy to the Grantee.

Q. Unauthorized Use:

1. The Grantee shall fully defend and hold harmless the State and the Department from any suits, actions, damages, and costs of every name and description, including attorneys' fees, arising from or relating to violation or infringement of a trademark, copyright, patent, trade secret, or intellectual property right provided, however, that the foregoing obligation shall not apply to the Department's misuse or modification of the Grantee's products or the Department's operation or use of the Grantee's products in a manner not contemplated by the Agreement. The Department will not be liable for any royalties.

2. The Grantee shall not be liable for any cost, expense, or compromise incurred or made by the State or the Department in any legal action without the Grantee's prior written consent, which

shall not be unreasonably withheld. The State and the Department shall have the right, at its own cost and expense, to participate in all actions under this Section Q.

3. For the avoidance of doubt, as the Grantee is a subdivision, as defined in section 768.28(2), F.S., pursuant to section 768.28(19), F.S., neither Party indemnifies nor insures or assumes any liability to the other Party for the other Party's negligence. Notwithstanding anything to the contrary in this Section Q., liability of either Party for tort claims is limited to the amounts prescribed in section 768.28, F.S., plus the Party's reasonable attorneys' fees.

R. Limitation of Liability:

1. Unless otherwise specifically enumerated in this Agreement, no Party shall be liable to the other Party for special, indirect, punitive, or consequential damages, including lost data or records (unless this Agreement requires the Grantee to back-up data or records), even if the Party has been advised that such damages are possible. No Party shall be liable to the other Party for lost profits, lost revenue, or lost institutional operating savings. The State and the Department may, in addition to other remedies available to them at law or in equity and upon notice to the Grantee, retain such monies from amounts due the Grantee as may be necessary to satisfy any claim for damages, penalties, costs, and the like asserted by or against them. Except as otherwise provided in this Agreement or the Data Sharing Agreement or its attachments or Riders, the Department is not liable for unauthorized access to information except as directly attributable to the actions of the Department. For all claims against Grantee under this Agreement, and regardless of the basis on which the claim is made, Grantee's liability under this Agreement for direct damages shall be limited to the dollar value of this Agreement. This limitation shall not apply to claims arising under Section Q. of this Agreement.

2. Pursuant to Section 200 of the 2024-2025 General Appropriations Act, the State is hereby released from all liability related to cybersecurity incidents impacting the Grantee.

S. Force Majeure and Notice of Delay from Force Majeure:

Neither Party shall be liable to the other for any delay or failure to perform under this Agreement if such delay or failure is neither the fault nor caused by the negligence of the Party or its employees or agents and the delay is due directly to acts of God, wars, acts of public enemies, strikes, fires, floods, or other similar cause wholly beyond the Party's control, or for any of the foregoing that affects subrecipients, contractors, or suppliers if no alternate source of supply is available. However, in the event a delay arises from the foregoing causes, the Party shall take all reasonable measures to mitigate any and all resulting damages, costs, delays, or disruptions to the project in accordance with the Party's performance requirements under this Agreement.

In the case of any delay the Grantee believes is excusable under this section, the Grantee shall provide written notice to the Department describing the delay or potential delay and the cause of the delay within: ten (10) calendar days after the cause that creates or will create the delay first arose (if the Grantee could reasonably foresee that a delay could occur as a result); or five (5) calendar days after the date the Grantee first had reason to believe that a delay could result (if the delay is not reasonably foreseeable). **THE FOREGOING SHALL CONSTITUTE THE**

GRANTEE'S SOLE REMEDY OR EXCUSE WITH RESPECT TO DELAY. Providing notice in strict accordance with this section is a condition precedent to such remedy.

The Department, in its sole discretion, will determine if the delay is excusable under this section and will notify the Grantee of its decision in writing. The Grantee shall not assert a claim for damages, other than for an extension of time, against the Department. The Grantee will not be entitled to an increase in the Agreement price or payment of any kind from the Department for any reason. If performance is suspended or delayed, in whole or in part, due to any of the causes described in this section, after the causes have ceased to exist, the Grantee shall resume performance, unless the Department determines, in its sole discretion, that the delay will significantly impair the ability of the Grantee to timely complete its obligations under this Agreement, in which case, the Department may terminate this Agreement in whole or in part.

T. Mandatory Disclosure Requirements:

1. Convicted Vendor List. The Grantee has a continuous duty to disclose to the Department if the Grantee or any of its affiliates, as defined by section 287.133(1)(a), F.S., are placed on the convicted vendor list. Pursuant to section 287.133(2)(a), F.S.: "A person or affiliate who has been placed on the convicted vendor list following a conviction for a public entity crime may not submit a bid, proposal, or reply on a contract to provide any goods or services to a public entity; may not submit a bid, proposal, or reply on a contract with a public entity for the construction or repair of a public building or public work; may not submit bids, proposals, or replies on leases of real property to a public entity; may not be awarded or perform work as a contractor, supplier, subcontractor, or consultant under a contract with any public entity; and may not transact business with any public entity in excess of the threshold amount provided in s. 287.017, F.S., for CATEGORY TWO for a period of 36 months following the date of being placed on the convicted vendor list."

2. Discriminatory Vendor List. The Grantee has a continuous duty to disclose to the Department if the Grantee or any of its affiliates, as defined by section 287.134(1)(a), F.S., are placed on the discriminatory vendor list. Pursuant to section 287.134(2)(a), F.S.: "An entity or affiliate who has been placed on the discriminatory vendor list may not submit a bid, proposal, or reply on a contract to provide any goods or services to a public entity; may not submit a bid, proposal, or reply on a contract with a public entity for the construction or repair of a public building or public work; may not submit bids, proposals, or replies on leases of real property to a public entity; may not be awarded or perform work as a contractor, supplier, subcontractor, or consultant under a contract with any public entity; and may not transact business with any public entity."

3. Antitrust Violator Vendor List. The Grantee has a continuous duty to disclose to the Department if the Grantee or any of its affiliates, as defined by section 287.137(1)(a), F.S., are placed on the antitrust violator vendor list. Pursuant to section 287.137(2)(a), F.S.: "A person or an affiliate who has been placed on the antitrust violator vendor list following a conviction or being held civilly liable for an antitrust violation may not submit a bid, proposal, or reply for any new contract to provide any goods or services to a public entity; may not submit a bid, proposal, or reply for a new contract with a public entity for the construction or repair of a public building or public work; may not submit a bid, proposal, or reply on new

leases of real property to a public entity; may not be awarded or perform work as a contractor, supplier, subcontractor, or consultant under a new contract with a public entity; and may not transact new business with a public entity."

4. Foreign Gifts and Contracts. The Grantee shall comply with any applicable disclosure requirements in section 286.101, F.S. Pursuant to section 268.101(7), F.S.: "In addition to any fine assessed under [section 286.101(7)(a), F.S.], a final order determining a third or subsequent violation by an entity other than a state agency or political subdivision shall automatically disqualify the entity from eligibility for any grant or contract funded by a state agency or any political subdivision until such ineligibility is lifted by the Administration Commission for good cause."

REMAINDER OF PAGE INTENTIONALLY LEFT BLANK

IN WITNESS WHEREOF, the Parties agree to the terms and conditions of this Agreement and have duly authorized their respective representatives to sign it on the dates indicated below.

Polk County:

By: _____

Name: William D. Beasley

Title: County Manager

Date: 4/27/2024

Department of Management Services:

By: _____

Name: _____

Title: _____

Date: _____

ATTACHMENT A
SOLUTION STATEMENT OF WORK

1. **Scope of Work.**

Pursuant to Section 200, FY 24-25 General Appropriations Act (GAA), the Parties agree that the Department shall, on behalf of the Grantee, expend funds for the provision of services, licenses, or commodities awarded to the Grantee to be utilized for the development and enhancement of cybersecurity risk management programs. The Grantee is being granted assistance in the form of services, licenses, or commodities to enhance its cybersecurity framework, to identify and mitigate risks, and to protect its infrastructure from threats through Florida's Local Government Cybersecurity Grant Program (the "Project").

2. **Awarded Capabilities.**

The Department shall offer the following capabilities/solutions to the Grantee:

Network-Based Asset Discovery: Armis
Endpoint Detection and Response: CrowdStrike
Security Operations Platform: Reliaquest GreyMatter
Email Security: Proofpoint

Note: The Department will make its best effort to award the Grantee's preferred solution per capability. However, the Department can only contract for a limited number of solutions based on best value, technical acceptability, and operational volume.

3. **Grantee Responsibilities.**

The Grantee shall complete the Project in accordance with the requirements set forth in this Agreement and any applicable local, State, and federal laws and regulations. The Grantee is solely responsible for ensuring that any provided solutions are compliant with applicable state and federal laws and regulations based on Grantee's intended use, including, but not limited to, Health Insurance Portability and Accountability Act, Family Educational Rights and Privacy Act, Driver Privacy Protection Act, and General Data Protection Regulation.

4. **Department Responsibilities.**

The Department shall review Grantee reports and other records and reconcile them to ensure that the requirements of section 215.971, F.S., pertaining to agreements funded with State financial assistance are fulfilled.

5. **Deliverables.**

The Grantee shall complete the following deliverable(s):

Deliverables		
No.	**Tasks**	**Performance Measures and Due Dates**
1	Execute this Grant Agreement.	The Grantee must execute the Grant Agreement within 45 calendar days of award.

2	Participate in a kick-off meeting with FL[DS] and the solution provider, if implementation is required.	The Grantee shall participate in the kick-off meeting with FL[DS] and the solution provider within five (5) calendar days of Purchase Order (PO) issuance.
3	Approve Final Implementation Plan(s) for solutions awarded, if implementation is required.	The Grantee must coordinate with the solution provider(s) to review the Implementation Plan(s). **If the Grantee chooses to proceed with a solution**, the Grantee must approve the Final Implementation Plan within 15 calendar days of PO issuance.
4	Complete all tasks in accordance with the Final Implementation Plan(s), if implementation is required.	The Grantee shall provide all necessary resources to execute tasks assigned to the Grantee in the Final Implementation Plan(s).
5	Notify the Department's Grant Manager of implementation completion per the Final Implementation Plan, if implementation is required.	The Grantee shall notify the Department's Grant Manager in writing within 10 calendar days of implementation completion.
6	Provide FL[DS] with any information related to this Agreement as requested by FL[DS].	The Grantee shall respond within seven (7) calendar days of any request from FL[DS].

6. Reporting Requirements.

The Department may request status meetings for the Grantee to report on the implementation, service, training, or support status, as necessary, with the Grantee's Grant Manager.

The Department may, at its sole discretion, develop a format and deadlines the Grantee must comply with when reporting the information above. The Grantee's failure to confirm completion of the Final Implementation Plan(s) or comply with the reporting format and schedule may result in termination of the awarded solutions.

7. Performance Standards.

The Grantee shall timely perform all tasks and provide deliverables as set forth in this Agreement. The Department is entitled at all times, upon request, to be advised as to the status of work being done by the Grantee, on behalf of the grantee, and the details thereof.

If the Department determines that there is a performance deficiency that requires correction by the Grantee, then the Department shall notify the Grantee. The Grantee shall make the correction within a timeframe specified by the Department. The Grantee shall provide the Department with a corrective action plan describing how the Grantee will address all performance deficiencies identified by the Department. If the corrective action plan is unacceptable to, or implementation of the plan fails to remedy the performance deficiencies, the Grantee shall work cooperatively with the Department to modify the corrective action plan or to remedy the deficiencies. Additionally, if a performance deficiency is attributable to the performance of a contractor or subcontractor of the Grantee, the Grantee shall take all actions available to it to enforce financial consequences in its contract with the contractor or subcontractor or to pursue damages.

8. Financial Consequences for Failure to Timely and Satisfactorily Perform.

Violations of this Agreement or applicable licenses, or failure to provide the deliverables, may result, except as detailed above, in termination of access to awarded solutions and require immediate removal of all software, hardware, or related services. Grantee may be subject to financial assessments related to such violations.

This provision for financial consequences shall not affect the Department's right to terminate the Agreement as provided elsewhere in the Agreement.

REMAINDER OF PAGE INTENTIONALLY LEFT BLANK

Department of Financial Services
Division of Accounting and Auditing – Bureau of Auditing

AUDIT REQUIREMENTS FOR AWARDS OF STATE AND FEDERAL FINANCIAL ASSISTANCE

The administration of resources awarded by the Department of Management Services (Department) to the Grantee may be subject to audits and/or monitoring by the Department, as described in this section.

MONITORING

In addition to reviews of audits conducted in accordance with 2 CFR 200, Subpart F - Audit Requirements, and section 215.97, Florida Statutes (F.S.), as revised (see AUDITS below), monitoring procedures may include, but not be limited to, on-site visits by Department staff, limited scope audits as defined by 2 CFR §200.425, or other procedures. By entering into this agreement, the Grantee agrees to comply and cooperate with any monitoring procedures or processes deemed appropriate by the Department. In the event the Department determines that a limited scope audit of the Grantee is appropriate, the Grantee agrees to comply with any additional instructions provided by Department staff to the Grantee regarding such audit. The Grantee further agrees to comply and cooperate with any inspections, reviews, investigations, or audits deemed necessary by the Chief Financial Officer (CFO) or Auditor General.

AUDITS

Part I: Federally Funded

This part is applicable if the Grantee is a state or local government or a nonprofit organization as defined in 2 CFR §200.90, §200.64, and §200.70.

1. A Grantee that expends $750,000 or more in federal awards in its fiscal year must have a single or program-specific audit conducted in accordance with the provisions of 2 CFR 200, Subpart F - Audit Requirements. EXHIBIT 1 to this form lists the federal resources awarded through the Department by this agreement. In determining the federal awards expended in its fiscal year, the Grantee shall consider all sources of federal awards, including federal resources received from the Department. The determination of amounts of federal awards expended should be in accordance with the guidelines established in 2 CFR §§200.502-503. An audit of the Grantee conducted by the Auditor General in accordance with the provisions of 2 CFR §200.514 will meet the requirements of this Part.
2. For the audit requirements addressed in Part I, paragraph 1, the Grantee shall fulfill the requirements relative to auditee responsibilities as provided in 2 CFR §§200.508-512.
3. A Grantee that expends less than $750,000 in federal awards in its fiscal year is not required to have an audit conducted in accordance with the provisions of 2 CFR 200, Subpart F - Audit Requirements. If the Grantee expends less than $750,000 in federal awards in its fiscal year and elects to have an audit conducted in accordance with the provisions of 2 CFR 200, Subpart F - Audit Requirements, the cost of the audit must be paid from non-federal resources (i.e., the cost of such an audit must be paid from Grantee resources obtained from other than federal entities).

Part II: State Funded

1. In the event that the Grantee expends a total amount of state financial assistance equal to or in excess of $750,000 in any fiscal year of such Grantee (for fiscal years ending June 30,

2017, and thereafter), the Grantee must have a state single or project-specific audit for such fiscal year in accordance with section 215.97, F.S.; Rule Chapter 69I-5, F.A.C., State Financial Assistance; and Chapters 10.550 (local governmental entities) and 10.650 (nonprofit and for-profit organizations), Rules of the Auditor General. EXHIBIT 1 to this form lists the state financial assistance awarded through the Department this agreement. In determining the state financial assistance expended in its fiscal year, the Grantee shall consider all sources of state financial assistance, including state financial assistance received from the Department, other state agencies, and other nonstate entities. State financial assistance does not include federal direct or pass-through awards and resources received by a nonstate entity for federal program matching requirements.

2. For the audit requirements addressed in Part II, paragraph 1, the Grantee shall ensure that the audit complies with the requirements of section 215.97(8), F.S. This includes submission of a financial reporting package as defined by section 215.97(2), F.S., and Chapters 10.550 (local governmental entities) and 10.650 (nonprofit and for-profit organizations), Rules of the Auditor General.

3. If the Grantee expends less than $750,000 in state financial assistance in its fiscal year (for fiscal years ending June 30, 2017, and thereafter), an audit conducted in accordance with the provisions of section 215.97, F.S., is not required. If the Grantee expends less than $750,000 in state financial assistance in its fiscal year and elects to have an audit conducted in accordance with the provisions of section 215.97, F.S., the cost of the audit must be paid from the nonstate entity's resources (i.e., the cost of such an audit must be paid from the Grantee's resources obtained from other than state entities).

Part III: Other Audit Requirements

N/A

Part IV: Report Submission

1. Copies of reporting packages for audits conducted in accordance with 2 CFR 200, Subpart F - Audit Requirements, and required by Part I of this form shall be submitted, when required by 2 CFR §200.512, by or on behalf of the Grantee directly to the Federal Audit Clearinghouse (FAC) as provided in 2 CFR §200.36 and §200.512.

   The FAC's website provides a data entry system and required forms for submitting the single audit reporting package. Updates to the location of the FAC and data entry system may be found at the OMB website.

2. Copies of financial reporting packages required by Part II of this form shall be submitted by or on behalf of the Grantee directly to each of the following:

   a. The Department at each of the following addresses:

      Electronic copies (preferred): Cybersecuritygrants@digital.fl.gov

      or

Paper copies:
Procurement & Grants Administrator
Florida Digital Service
Department of Management Services
2555 Shumard Oaks Blvd, Suite 200
Tallahassee, Florida 32399

b. The Auditor General's Office at the following address:

Auditor General
Local Government Audits/342
Claude Pepper Building, Room 401
111 West Madison Street
Tallahassee, Florida 32399-1450

The Auditor General's website (https://flauditor.gov/) provides instructions for filing an electronic copy of a financial reporting package.

3. Any reports, management letters, or other information required to be submitted to the Department pursuant to this agreement shall be submitted timely in accordance with 2 CFR §200.512, section 215.97, F.S., and Chapters 10.550 (local governmental entities) and 10.650 (nonprofit and for-profit organizations), Rules of the Auditor General, as applicable.

4. Grantees, when submitting financial reporting packages to the Department for audits done in accordance with 2 CFR 200, Subpart F - Audit Requirements, or Chapters 10.550 (local governmental entities) and 10.650 (nonprofit and for-profit organizations), Rules of the Auditor General, should indicate the date that the reporting package was delivered to the Grantee in correspondence accompanying the reporting package.

Part V: Record Retention

The Grantee shall retain sufficient records demonstrating its compliance with the terms of the award(s) and this agreement for a period of five (5) years from the date the audit report is issued, and shall allow the Department, or its designee, the CFO, or Auditor General access to such records upon request. The Grantee shall ensure that audit working papers are made available to the Department, or its designee, the CFO, or Auditor General upon request for a period of five (5) years from the date the audit report is issued, unless extended in writing by the Department.

EXHIBIT 1

Federal Resources Awarded to the Grantee Pursuant to this Agreement Consist of the Following:

1. Federal Program A:

   N/A

2. Federal Program B:

   N/A

Compliance Requirements Applicable to the Federal Resources Awarded Pursuant to this Agreement are as Follows:

1. Federal Program A:

   N/A

2. Federal Program B:

   N/A

State Resources Awarded to the Grantee Pursuant to this Agreement Consist of the Following:

Matching Resources for Federal Programs:

1. Federal Program A:

   N/A

2. Federal Program B:

   N/A

Subject to Section 215.97, F.S.:

1. State Project A: Local Government Cybersecurity Grant

   State Awarding Agency: Florida Department of Management Services

   Catalog of State Financial Assistance Title and Number: 72.016

   Amount: $_____

2. State Project B:

   N/A

Compliance Requirements Applicable to State Resources Awarded Pursuant to this Agreement Are as Follows:

The compliance requirements are as stated in Grant Agreement No. DMS-24/25-145 between the Grantee and the Department, entered in State Fiscal Year 2024-25.

ATTACHMENT C
GRANTEE DATA SHARING AGREEMENT

Purposes

Grantee desires to utilize software licenses, applications, and solutions, as applicable, in connection with the attached Exhibit A – Cybersecurity Incident Response Rider and Exhibit B – Solution Rider, incorporated herein. This DSA describes the terms and conditions for the use of software licenses, applications, and solutions and protection of Covered Data, including requirements to safeguard the availability, confidentiality, and integrity of Covered Data in furtherance of the security objectives of Chapter 282, F.S.

I. Definitions

A. Access – The authorization to inspect, review, transmit, duplicate, communicate with, retrieve data from, or otherwise make use of any Covered Data, regardless of type, form, or nature of storage. "Access" to a computer system or network includes local and remote access, as applicable.

B. Authorized Purpose – The purpose(s) for which an Authorized Third Party may access, use, or disclose the Covered Data.

C. Authorized Third Party – An individual, state agency, other Florida state or local governmental entity, or a private sector contractor or service provider of the Grantee which receives Covered Data.

D. Authorized User – An individual granted Access or to use Software Entitlement by either FL[DS] or Grantee.

E. County and Municipality Cybersecurity Technical Assistance Program ("the Program") – refers to the grant program established by the 2024-2025 General Appropriations Act to enhance county and municipal cybersecurity and protect the infrastructure of local governments from threats.

F. Covered Data – The limited subset of security data that is derived from Grantee's use of any Software Entitlements as defined in the attached Rider(s); a Grantee's confidential or proprietary information; and personal information as defined under section 501.171, F.S., and any other applicable privacy or data breach notification laws as may exist.

G. Data Breach – Either (1) any unauthorized access to, or use or disclosure of, Covered Data for any purpose other than as expressly permitted by this DSA or required by law; or (2) a breach of privacy or of the security of the Covered Data. Good faith access of data by an employee or agent of the Grantee does not constitute a breach of security, provided that the information is not used for a purpose unrelated to the business or subject to further unauthorized use.

H. DSA Coordinators – The individuals appointed by the signatories to this DSA as the point of contact for this DSA, who are responsible for ensuring that the Authorized Users comply with the activities identified herein.

I. HIPAA - Health Insurance Portability and Accountability Act of 1996.

J. Information Technology (IT) Coordinators – The individuals appointed by the signatories to this DSA as responsible for data flow and other technology-related considerations under this DSA.

K. Information Technology Resources – As defined in section 282.0041, Florida Statutes, the data processing hardware and software and services, communications, supplies, personnel, facility

resources, maintenance, and training. As used in this DSA, the term also includes the definition for "Information Technology," as defined in section 282.0041, Florida Statutes, to add equipment, hardware, software, firmware, programs, systems, networks, infrastructure, media, and related material used to automatically, electronically, and wirelessly collect, receive, access, transmit, display, store, record, retrieve, analyze, evaluate, process, classify, manipulate, manage, assimilate, control, communicate, exchange, convert, converge, interface, switch, or disseminate information of any kind or form.

L. Software Entitlement – Proprietary software provided to the Grantee under the Agreement to satisfy provision of the solution(s) awarded to the Grantee, as identified in Attachment A – Solution Statement of Work.

II. Responsibilities of the Parties

A. **Data Transmission**. Covered Data shall only be transmitted through secure file transfer protocol or other secure transmission methods utilizing a National Institute of Standards and Technology approved means of electronic encryption as well as password protection and in a file format and layout determined by FL[DS]. Covered Data shall not be transmitted via any other means, including electronic mail. If applicable to any transmission of the Covered Data, both transmitting and receiving Grantee shall completely and permanently remove Covered Data from any temporary transfer location within twenty-four (24) hours of receipt of the Covered Data.

B. **Compliance with Applicable Laws**. Each Party covenants and agrees that, in the performance of this DSA, it shall comply with all applicable federal, state, and local laws, statutes, and regulations including, but not limited to, such laws set forth in Article VI as applicable to a Project and such other data privacy or security laws, all as they exist now and as they may be amended from time to time ("Applicable Laws"). In the event of any notice of a material violation of Applicable Laws, or an investigation into an alleged material violation, the affected Party shall promptly notify the other in writing of such notice.

The Parties further agree to follow and be bound by the terms and conditions of any policy decisions or directives from the federal and state agencies with jurisdiction over the use of the data described herein upon receipt of written notice directing that such rules, policy decisions, or directives apply to this DSA.

C. **HIPAA Business Associate Agreement.** To the extent that a Party is acting as a Business Associate (as defined by HIPAA) of the other Party, the Parties further agree to enter into a Business Associate Agreement as necessary, in the form of a mutually agreed-upon appendix to the DSA.

D. **Incorporation and Compliance with Exhibits, Appendices and Riders, if Applicable.** The Project Riders, and any exhibits or appendices to this DSA are hereby incorporated and made a part hereof and are an integral part of this DSA. Each Rider, Exhibit, and Appendix attached hereto or referred to herein are hereby incorporated in and made a part of this DSA as if set forth in full herein.

III. FL[DS] Role and Responsibilities

A. FL[DS] is responsible for:

1. Processing Covered Data in accordance with the State Cybersecurity Act;

2. Facilitating data sharing with the Grantee and/or an Authorized Third Party in accordance with this DSA;

3. Providing the Grantee with the option to utilize Software Entitlements; and

4. Protecting the integrity of Covered Data obtained by FL[DS] through Grantee's use of any of the Software Entitlements. FL[DS] will not disclose this Covered Data to any third party unless required by law or as otherwise authorized by Grantee.

B. FL[DS] will only access, use, or disclose Covered Data, as permitted by Grantee, as required by Applicable Law, or as necessary for completion of its responsibilities under this DSA, including any Project Riders. FL[DS] will ensure that its Authorized Users only access, use, or disclose Covered Data, as permitted by Grantee, as required by Applicable Law, or as necessary for completion of its responsibilities for any Projects, as assigned by FL[DS].

C. FL[DS] will exercise reasonable care and no less than the same degree of care FL[DS] uses to protect its own confidential information to prevent confidential information from being used in a manner that is not expressly a purpose authorized in this DSA or as required by Applicable Law.

IV. Grantee's Role and Responsibilities

A. Covered Data is and shall remain the property of Grantee.

B. Grantee is solely responsible for its Access to and use of Software Entitlements and Covered Data, including:

1. Ensuring a level of security appropriate to the risk in respect of Covered Data;

2. Securing Grantee's and its Authorized Users' systems and devices that can Access FL[DS] systems and Software Entitlements and complying with the Security Standards;

3. Selecting and/or ensuring that Grantee has selected its Authorized Users; activating and deactivating the Access, credentials, and privileges of its Authorized Users; and managing access controls to the FL[DS] system and Software Entitlements in a timely manner in accordance with the Security Standards;

4. Securing the account authentication credentials, systems, and devices of Grantee personnel who the Grantee designates to be Authorized Users;

5. Managing the compliance of its Authorized Users with the Grantee's established security measures and as required by Applicable Law;

6. Maintaining audit logs, as deemed necessary by the Grantee to demonstrate compliance with its obligations under this DSA;

7. Backing up Covered Data, if required by law or Grantee policy; and

8. Ensuring that it and its Authorized Users remain in compliance with the terms and conditions of any Software Entitlements.

C. FL[DS] is not responsible for, and has no obligation for:

1. Selecting or verifying Grantee's Authorized Users, activating or deactivating the Access or credentials of Authorized Users; or

2. Protecting Covered Data that Grantee elects to store or transfer outside of FL[DS]'s and its sub-processors' systems (for example, offline or on-premises storage).

V. Unauthorized Disclosure/Data Breach

A. In the event of a Data Breach of the Covered Data while in Grantee's (or an Authorized Third Party's) custody or control or as a result of Grantee's (or an Authorized Third Party's) access to or use of the Covered Data, which requires the provision of notice in accordance with section 501.171, F.S., or other Applicable Law (including, but not limited to, HIPAA), the Parties agree as follows:

1. Grantee shall notify FL[DS] of the Data Breach not more than 24 hours after discovery that a Data Breach has occurred or is reasonably likely to have occurred.

2. Grantee (or its Authorized Third Party) shall be responsible for all costs related to the Data Breach including FL[DS]' and/or Grantee's (or an Authorized Third Party's) costs of complying with all legal requirements, including the requirements for Data Breach notification under Applicable Law, as well as defending any claims, actions, or lawsuits related thereto.

3. If a Data Breach is subject to the notice provisions of section 501.171, F.S., or Applicable Law, the Parties agree to cooperate and work together to ensure full legal compliance and to provide breach notification to the extent required by Applicable Law. Grantee shall use its best and diligent efforts to identify the individuals entitled to receive notice of the Data Breach and obtain the names and mailing information of such individuals, so that FL[DS] and/or Grantee are able to distribute the notices within the legally required time periods. FL[DS] and/or Grantee, as applicable, shall bear its internal administrative and other costs incurred in identifying the affected individuals and their mailing information.

4. In the event of a Data Breach, including the privacy or security of the Covered Data, while in the custody or control of the Grantee, if the Grantee must provide notice as a result of the requirements contained in section 501.171, F.S., or other Applicable Law, the Grantee shall submit a draft of the notice to FL[DS] for prior review and approval of the contents of the notice, prior to disseminating the notice. Such approval shall not be unreasonably delayed or withheld.

B. If Grantee experiences a breach of the security of its systems that results in a breach of the security of FL[DS]'s systems ("FL[DS] Breach"), Grantee shall be responsible for all costs related to the FL[DS] Breach including FL[DS]'s costs of complying with all legal requirements, including any costs for data breach notification under section 501.171, F.S., or Applicable Law, as well as defending any claims, actions, or lawsuits against the FL[DS] related thereto. Grantee, at its own expense, shall cooperate fully with FL[DS] in the investigation, eradication, remediation, and recovery from the FL[DS] Breach.

C. If FL[DS] experiences a breach of the security of its systems that results in a breach of the security of Grantee's systems ("Grantee Breach"), FL[DS] shall be responsible for all costs related to the Grantee Breach including Grantee's costs of complying with all legal requirements, including the requirements for data breach notification under section 501.171, F.S., or Applicable Law, as well as defending any claims, actions or lawsuits related thereto. FL[DS], at its own expense, shall

cooperate fully with Grantee in the investigation, eradication, remediation, and recovery from the Grantee Breach.

D. If either FL[DS] or Grantee is obligated under this Section to pay costs incurred by the other Party, the Party required to pay such costs shall submit a draft of the legal notifications and other public communications to the other Party for prompt review and approval of the contents prior to disseminating the notification or communication. Such approval shall not be unreasonably delayed or withheld.

E. The Parties understand and agree the provisions of this DSA relating to the protection and security of the Covered Data constitute a material condition of this DSA. This Article V. Unauthorized Disclosure/Data Breach is subject to Sections Q. and R. of the Agreement.

VI. Additional Terms Applicable to Certain Circumstances.

A. Grantee is responsible for their Covered Data and entering into any required additional agreements related thereto. Grantee shall provide the FL[DS] DSA Coordinator with written notice prior to granting Access to any of the data types listed in subsections B-E, below, to FL[DS] or Software Entitlements. In the event of a conflict between the terms and conditions of this Article VI and the remainder of the DSA, the terms and conditions of Article VI shall control. Moreover, a Project may include the use of information described in more than one (1) of the provisions set forth in this Article VI, or it may include the use of information not described in this Article VI. In the event of a conflict between or among the terms and conditions of Subsections B, C, D or E of this Article VI, the more restrictive terms and conditions shall apply unless otherwise provided by Applicable Law or guidance by the applicable regulatory enforcement agencies or bodies.

B. **CJIS**. The terms and conditions of this Article VI.B. apply when Covered Data involved in a Project includes criminal justice information.

1. CJIS Covered Data. Covered Data may also include, but shall not be limited to, CJIS Covered Data. For purposes of this DSA, CJIS Covered Data shall mean criminal justice information that is provided by the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) system and that is necessary for law enforcement and civil agencies to perform their missions, including, but not limited to, biometric, identity history, biographic, property, and case/incident history data.

2. Disclosure of CJIS Covered Data. The disclosure of CJIS Covered Data under the DSA, as modified by this section, is governed by the CJIS Security Policy, available at https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center. In accordance with the CJIS Security Policy and 28 CFR Part 20, use of the CJIS system under the DSA is restricted to: detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, rehabilitation of accused persons or criminal offenders, and other legally authorized purposes.

3. Training. The Parties agree to work together to provide Authorized Users with confidentiality, privacy, and security training regarding access, use, and disclosure requirements for the CJIS Covered Data under the CJIS Security Policy.

4. Access Requirements. Unique authorization is required for Access to the CJIS Covered Data and must be properly authenticated and recorded for audit purposes, including CJIS security and other applicable audit requirements.

C. **HIPAA and State Protected Health Information.** The terms and conditions of this Article VI.C. apply when Covered Data involved in a Project includes protected health information (PHI) and such other sensitive health information, the disclosure of which may be limited or restricted by law, including, but not limited to, mental health and drug and alcohol related information.

1. PHI Covered Data. Covered Data may also include, but shall not be limited to, PHI Covered Data. For purposes of this DSA, "PHI Covered Data" shall mean "protected health information" or "PHI," as such term is defined by HIPAA. PHI shall include, but shall not be limited to, any other medical or health-related information that is afforded greater protection under more restrictive federal or state law, including, but not limited to, the Substance Abuse and Mental Health Services Act (SAMSHA), located at 42 C.F.R. Part 2, the Florida Mental Health Act (the Baker Act), located at Fla. Stat. § 394.451 – 394.47892, and the Hal S. Marchman Alcohol and Other Drug Services Act, located at Fla. Stat. § 397.301 et seq.

2. Disclosure of PHI Covered Data. The disclosure of PHI Covered Data under the DSA, as modified by this Article C, is governed by HIPAA and more restrictive federal or state law, as applicable. Accordingly, the disclosure of PHI Covered Data under the DSA is permitted only with the consent of the individual who is the subject of the PHI Covered Data, by court order that meets the requirements of applicable law, and for other purposes as permitted by Applicable Law.

3. Business Associate Agreement. To the extent that FL[DS] is a "Business Associate" of Grantee, as such term is defined under HIPAA, the Parties agree to enter into a mutually agreeable Business Associate Agreement.

4. Training. The Parties agree to work together to provide Authorized Users with confidentiality, privacy, and security training regarding access, use, and disclosure requirements for the PHI Covered Data under HIPAA and more restrictive federal or state law, to the extent applicable.

5. Access Requirements. Unique authorization is required for Access and must be properly authenticated and recorded for audit purposes, including HIPAA audit requirements and other audit requirements under more restrictive federal or state law, to the extent applicable.

D. **FERPA**. The terms and conditions of this Article VI.D. apply when Covered Data includes student education records as defined by the Family Educational Rights and Privacy Act, 20 USC §1232g, and its implementing regulations set forth at 34 CFR Part 99 (collectively, "FERPA").

1. FERPA Covered Data. Covered Data may also include, but shall not be limited to, FERPA Covered Data. For purposes of this DSA, "FERPA Covered Data" shall mean student education records as defined by FERPA.

2. Disclosure of FERPA Covered Data. The disclosure of FERPA Covered Data under the DSA, as modified by this section, is governed by FERPA. Accordingly, the disclosure of FERPA Covered Data under the DSA is permitted with parent or eligible student consent and, without such consent, in the following circumstances: (i) to school officials with legitimate educational interest; (ii) to other schools to which a student is transferring; (iii) to specified officials for audit or evaluation purposes; (iv) to appropriate parties in connection with financial aid to a student; (v) to organizations conducting certain studies for or on behalf of the school; (vi) to accrediting organizations; (vii) to comply with a judicial order or lawfully issued subpoena; (viii) to appropriate officials in cases of health and safety emergencies; (ix) to state and local authorities, within a juvenile justice system, pursuant to specific state law; and (x) as otherwise provided by FERPA.

3. Training. The Parties agree to work together to provide Authorized Users with confidentiality, privacy, and security training regarding access, use, and disclosure requirements for the FERPA Covered Data under FERPA.

4. Access Requirements. Unique authorization is required for Access and must be properly authenticated and recorded for audit purposes, including FERPA and any other applicable audit requirements.

E. **DPPA**. The terms and conditions of this Article VI.E. apply when Covered Data includes motor vehicle record information.

1. DPPA Covered Data. For purposes of the DSA, Covered Data may include, but shall not be limited to, DPPA Covered Data. For purposes of this DSA, "DPPA Covered Data" shall mean motor vehicle information as set forth in the Driver Privacy Protection Act, 18 U.S.C. § 2721 ("DPPA").

2. Disclosure of DPPA Covered Data. The disclosure of DPPA Covered Data under the DSA, as modified by this section, is governed by DPPA. DPPA prohibits the disclosure of personal information, as defined in 18 U.S.C. § 2725(3), that is contained in motor vehicle records, but such information may be used by any government agency, such as FL[DS] and Grantee, in carrying out its functions. Such personal information may not be re-disclosed by FL[DS] or Grantee, however, except in accordance with the permissible uses set forth at 18 U.S.C. § 2721(b). With certain limited exceptions, DPPA further prohibits the disclosure of highly restricted personal information, as defined in 18 U.S.C. § 2725(4), without the express consent of the individual who is the subject of such information. In accordance with section 119.0712(2)(d)(2), F.S., the emergency contact information contained in a motor vehicle record, without the express consent of the person to whom such emergency contact information applies, may be released only to: (a) law enforcement agencies for purposes of contacting those listed in the event of an emergency; or (b) a receiving facility, hospital, or licensed detoxification or addictions receiving facility pursuant to sections 394.463(2)(a) or 397.6772(1)(a), F.S., for the sole purpose of informing a patient's emergency contacts of the patient's whereabouts. E-mail addresses that are collected by the Florida Department of Highway Safety and Motor Vehicles also may not be disclosed pursuant to Section 119.0712(2)(c), F.S.

3. Training. The Parties agree to work together to provide Authorized Users with confidentiality, privacy, and security training regarding access, use, and disclosure requirements for the DPPA Covered Data under DPPA and the Florida Statutes referenced above.

4. Access Requirements. Unique authorization is required for Access and must be properly authenticated and recorded for audit purposes, including, but not limited to, compliance with these terms and conditions.

VII. Designation of DSA Coordinators

A. The Coordinators for this DSA are:

FL[DS] DSA Coordinator:

Policy Manager
2555 Shumard Oak Boulevard
Tallahassee, FL 32399

Telephone: 850-413-0604
Email: Policy@digital.fl.gov

FL[DS] IT Coordinator:

State Cybersecurity Information Security Officer
2555 Shumard Oak Boulevard
Tallahassee, FL 32399
Telephone: 850-413-0604
Email: Cyber@digital.fl.gov

Grantee's DSA Coordinator:

James Loughlin
Polk County
330 W. Church St.
Bartow, Florida 33830
Telephone: +1 (863) 534-7564
Email: jamesloughlin@polk-county.net

Grantee's IT Coordinator:

David Palmer
Polk County
330 W. Church St.
Bartow, Florida 33830
Telephone: +1 (863) 534-7660
Email: davidpalmer@polk-county.net

B. Changes to the DSA and/or IT Coordinator designations may be accomplished by providing email change notification that is acknowledged by both Parties.

VIII. Inspection of Records

Each Party shall permit the other Party and any other applicable state and federal representatives with regulatory oversight over the other Party, or their designees, to conduct inspections described in this paragraph, or to make on-site inspections of records relevant to this DSA to ensure compliance with any state and federal law, regulation, or rule. Such inspections may take place with notice during normal business hours wherever the records are maintained. Each Party shall ensure a system is maintained that is sufficient to permit an audit of such Party's compliance with this DSA and the requirements specified above. Failure to allow such inspections constitutes a material breach of this DSA. This DSA may be terminated in accordance with Article VII.C. for a material breach.

IX. Grantee Additional Terms

A. Contractors. Grantee shall ensure all contractors that have Access to Covered Data or Software Entitlements comply with all requirements of this DSA. The Software Entitlements shall not be Accessible by, or deployed on, Information Technology Resources not owned, employed, or controlled by Grantee.

RELEVANT FLORIDA STATUTES (2022)

Section 282.3185, Florida Statutes (F.S.), the "Local Government Cybersecurity Act," directs the Florida Digital Service (FL[DS]) to provide training in cybersecurity to local governments, oversee their compliance in adopting cybersecurity standards, and to receive cybersecurity incident and ransomware event notifications through the State Cybersecurity Operations Center. Such incident reporting must also include "[a] statement requesting or declining assistance from the Cybersecurity Operations Center, the Cybercrime Office of the Department of Law Enforcement, or the sheriff who has jurisdiction over the local government." per section 282.3185, F.S.

Under Section 200 of the 2024-2025 General Appropriations Act, FL[DS] has been directed to provide nonrecurring assistance to local governments for the development and enhancement of cybersecurity risk management programs.

Section 119.0725, F.S., establishes that coverage limits and deductible or self-insurance amounts of insurance or other risk mitigation coverages acquired for the protection of information technology systems, operational technology systems, or data of entities subject to the requirements of section 119.07(1), F.S., and section 24(a), Article I of the State Constitution; information relating to existing or proposed information technology and operational technology systems and assets, whether physical or virtual, the incapacity or destruction of which would negatively affect security, economic security, public health, or public safety; cybersecurity incident information reported under section 282.3185, F.S.; network schematics, hardware and software configurations, or encryption information or information that identifies detection, investigation, or response practices for suspected or confirmed cybersecurity incidents, including suspected or confirmed breaches, if the disclosure of such information would facilitate unauthorized access to or unauthorized modification, disclosure, or destruction of data or information, whether physical or virtual, or information technology resources, which include an agency's existing or proposed information technology systems; and the recordings and transcripts of public meetings where such information may be revealed are confidential and exempt, and such public meetings are exempt from section 286.011, F.S., and section 24(b), Article I of the State Constitution.

Exhibit A
Cybersecurity Incident Response Rider

I. Definitions

In addition to the defined terms in the DSA, capitalized terms used herein have the meanings provided below:

A. Cloud Console – The global administrative accounts for Software Entitlements directly managed and licensed by FL[DS].

B. Customer Account – The accounts for Software Entitlements directly utilized by Grantee.

C. Information Technology Resources – As defined in section 282.0041, Florida Statutes, data processing hardware and software and services, communications, supplies, personnel, facility resources, maintenance, and training. As used in this IR Rider, the term also includes the definition for "Information Technology," as defined in section 282.0041, Florida Statutes, to add equipment, hardware, software, firmware, programs, systems, networks, infrastructure, media, and related material used to automatically, electronically, and wirelessly collect, receive, access, transmit, display, store, record, retrieve, analyze, evaluate, process, classify, manipulate, manage, assimilate, control, communicate, exchange, convert, converge, interface, switch, or disseminate information of any kind or form.

D. Managing Organization – The entity managing the use of the Software Entitlements and their Cloud Consoles. As used in this IR Rider, the Managing Organization is FL[DS].

E. Protected Grantee Data – Data, not including Telemetry Data, maintained and generated by Grantee, which shall not be Accessed or Accessible by, or sent to, Software Entitlements.

F. Solution Data – Data, reports, or other information generated by Software Entitlements. This may be derived from, but does not include, Telemetry Data.

G. Telemetry Data – Data generated by Grantee through automated communication processes from multiple data sources and processed by Software Entitlements.

H. View - The permissions Grantee grants to FL[DS] to see Telemetry and Solutions Data provided to the Managing Organization by Customer Accounts. A View does not permit FL[DS] Access to Protected Grantee Data.

II. Purpose

FL[DS] and Grantee enter into this IR Rider to establish the terms and conditions for FL[DS] Access to assist Grantee with responding to incidents.

III. Incident Response

A. **Incident Response Support**. As specified in section 282.3185(5), F.S., if applicable, upon discovery of an incident, Grantee may request, or FL[DS] may offer to provide, incident response support. Access to Grantee Information Technology Resources shall be limited to the extent expressly agreed to by Grantee. Such Access and support are unilaterally terminable at any time by either Party. FL[DS] may establish, and Grantee shall comply with, protocols or procedures for reporting and requesting support for incidents under this IR Rider, responding to incidents, and the types of support available to be provided for an incident. Grantee shall mitigate the impact of the incident and

preserve all relevant documents, records, and data. Grantee shall cooperate and coordinate with FL[DS] in responding to incidents where incident response support is received, including, but not limited to:

1. Assisting with any incident response related investigation by FL[DS];
2. Providing FL[DS] with physical access to the affected facilities and operations;
3. Facilitating interviews with Grantee personnel; and
4. Making all relevant records, logs, files, data reporting, and other materials available to FL[DS] or Grantee-authorized third parties.

FL[DS] shall only Access Covered Data, other Grantee data, and Grantee Information Technology Resources as permitted by Grantee. Any specific limitations on such Access shall be documented.

Upon termination of each instance of incident response support, regardless of the reason for such termination, Grantee shall assist FL[DS] with any close-out or post-incident documentation upon request.

B. **Covered Data and Personally Identifiable Information**. FL[DS] will not disclose Covered Data or other data made Accessible during incident response support to any third party unless required by law or as authorized by Grantee. In the event such data is required by law to be disclosed, FL[DS] shall make best efforts to notify Grantee prior to such disclosure.

IV. FL[DS] Role and Responsibilities

FL[DS] shall provide Grantee with the option to utilize the Software Entitlements to enhance the Grantee's cybersecurity and protect the Grantee's infrastructure from threats.

FL[DS] will Access a View of the Telemetry Data and Solution Data. FL[DS] will only use Telemetry and Solutions Data for the purpose of developing and implementing the Program; identifying and responding to risks and incidents; and in furtherance of meeting FL[DS]' and Grantee's statutory and regulatory obligations. FL[DS] will not disclose the Telemetry Data and Solutions Data to any third party unless required by law or as otherwise authorized by Grantee. FL[DS] will provide incident response services and resources as allowed and agreed to by FL[DS] and Grantee in responding to risks and incident.

V. Grantee Roles and Responsibilities

Grantee shall cooperate with and provide all assistance necessary to FL[DS]' incident response support.

VI. Indemnification

For the avoidance of doubt, the Grantee agrees to indemnify FL[DS] and the Department for any claims related to this rider pursuant to the terms provided in Section Q., Unauthorized Use, of the Grant Agreement.

VII. Conflict

In the event of a conflict between this IR Rider, the DSA, and any other rider, the terms of this IR Rider shall control.

VIII. Liability and Termination of Incident Response Support

Except as described in the DSA or other riders, incident response services and resources of FL[DS] or Grantee-authorized third parties shall be provided by FL[DS] without warranty by, and without liability to, FL[DS] or such Grantee-authorized third parties. Upon request, FL[DS] or Grantee-authorized third parties shall provide reasonable assistance to return Grantee Information Technology Resources to the operational status prior to the involvement of FL[DS] incident response support.

REMAINDER OF PAGE INTENTIONALLY LEFT BLANK

Exhibit B
Solution Rider

I. Definitions

In addition to the defined terms in the DSA, capitalized terms used herein have the meanings provided below:

A. Protected Grantee Data – Data, not including Telemetry Data, maintained, and generated by Grantee, which shall not be Accessed or Accessible by, or sent to, the Licensed Software Solution.

B. Customer Account – The Licensed Software Solution account directly utilized by Grantee.

C. Local Government Cybersecurity Grant Program ("the Program") –The Program established by the 2024-2025 General Appropriations Act to provide nonrecurring assistance to local governments for the development and enhancement of cybersecurity risk management programs.

D. Licensed Software Solutions – Proprietary software provided to the Grantee under the Agreement to satisfy provision of the solution(s) awarded to the Grantee, as identified in Attachment A of the Grant Agreement.

E. Managing Organization – The entity managing the use of the Licensed Software Solution and its implementation. As used in this Rider, the Managing Organization is FL[DS].

F. Protected Grantee Data – Data, not including Telemetry Data, maintained, and generated by Grantee, which shall not be Accessed or Accessible by, or sent to, the Licensed Software Solution.

G. Solution Console – The global administrative account(s) directly managed and licensed by FL[DS] to provide the Grantee with the Software Entitlement.

H. Solution Data – Data, reports, or other information generated by the Licensed Software Solution. May be derived from but shall not include Telemetry Data.

I. Telemetry Data –The data generated by Grantee through automated communication processes from multiple data sources and processed by the Licensed Software Solution.

J. View – The permissions granted for FL[DS] to see Telemetry Data provided to the Managing Organization's Solution Console by the Customer Account. A View does not permit FL[DS] Access to Protected Grantee Data.

II. Statement of Work

A. **Purpose/Scope:** FL[DS] and Grantee enter into this Rider to establish the terms and conditions for Grantee Access to the Licensed Software Solution provided by FL[DS]; to establish the maintenance, use, and disclosure of the Telemetry Data generated by Grantee and uploaded to the Solution Console; and to provide terms and conditions for the use of the Licensed Software Solution.

B. **FL[DS] Role and Responsibilities**: FL[DS] is responsible for providing Grantee with the option to utilize the Licensed Software Solution.

FL[DS] shall be permitted to Access a View of the Telemetry Data provided within the Solution Console via permissions to the Customer Account.

FL[DS] will only use Telemetry Data for the express purpose of developing and implementing the Program and in furtherance of FL[DS]' and Grantee's statutory and regulatory obligations. FL[DS] will not disclose the Telemetry Data to any third party unless required by law or as otherwise authorized by Grantee.

C. **Grantee's Role and Responsibilities:** Grantee is responsible for:

   a. Grantee Access to and use of the Licensed Software Solution in compliance with all terms and conditions related thereto, including the Agreement terms and the vendor terms and conditions to be provided to the Grantee by FL[DS] without need for an amendment hereto by the Parties and which, after provision thereof, will be deemed incorporated herein and a material component hereof;

   b. Activating and deactivating the Access, credentials, and privileges of its authorized users;

   c. Ensuring no Protected Grantee Data is submitted to the Licensed Software Solution;

   d. Entering into any additional agreement with FL[DS], the Licensed Software Solution provider, or other third-parties as may be required by law regarding Protected Grantee Data, as applicable; and

   e. Managing access controls to allow View by FL[DS] and Access by the Licensed Software Solution.

   f. Telemetry Data, even as it may be housed, maintained, or processed by the Licensed Software Solution, is and shall remain the property of Grantee.

D. **Indemnification:** For the avoidance of doubt, the Grantee agrees to indemnify FL[DS] and the Department for any costs related to Grantee's use of the Licensed Software Solution pursuant to the terms provided in Section Q., Unauthorized Use, of the Grant Agreement.

E. **Conflict:** In the event of a conflict between this Rider and the DSA, the terms of this Rider shall control.

REMAINDER OF PAGE INTENTIONALLY LEFT BLANK