AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT

1. CONTRACT ID CODE	PAGE	OF PAGES
	1	11

2. AMENDMENT/MODIFICAITON NO.	3. EFFECTIVE DATE	4. REQUISITION/PURCHASE REQ. NO.	5. PROJECT NO. *(If applicble)*
22	04/25/2024		

6. ISSUED BY CODE SP4701

DLA Contracting Services Office - Philadelphia
700 Robbins Ave.
Philadelphia, PA 19111
Attn: R&D CONTRACTING TEAM

7. ADMINISTERED BY *(If other than Item 6)* CODE

SAME AS BLOCK 6

8. NAME AND ADDRESS OF CONTRACTOR *(No., street, county, State and ZIP Code)*

CODE FACILITY CODE

(X)

☒ 9A. AMENDMENT OF SOLICIATION NO. BAA0001-22

9B. DATED *(SEE ITEM 11)* 06/13/2022

☐ 10A. MODIFICATION OF CONTRACT/ORDER NO.

10B. DATED *(SEE ITEM 13)*

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

☒ The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offers ☐ is extended, ☒ is not extended.

Offers must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended, by one of the following methods: (a)By completing items 8 and 15, and returning _____ copies of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted; or (c) By separate letter or telegram which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment your desire to change an offer already submitted, such change may be made by telegram or letter, provided each telegram or letter makes reference to the solicitation and this amendment, and is received prior to the opening hour and date specified.

12. ACCOUNTING AND APPROPIRATION DATA *(If required)*

13. THIS ITEM ONLY APPLIES TO MODIFICATION OF CONTRACTS/ORDERS. IT MODIFIES THE CONTRACT/ORDER NO. AS DESCRIBED IN ITEM 14.

CHECK ONE	
☐	A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: *(Specify authority)* THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NO. IN ITEM 10A.
☐	B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES *(such as changes in paying office, appropriation date, etc.*) SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(b).
☐	C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF:
☐	D. OTHER *(Specify type of modification and authority)*

E. IMPORTANT: Contractor ☐ is not, ☐ is required to sign this document and return _____ copies to the issuing office.

14. DESCRIPTION OF AMENDMENT/MODIFICATION (*Organized by UCF section headings, including solicitation/contract subject matter where feasible.)*

See Continuation Pages.

Except as provided herein, all terms and conditions of the document referenced in Item 9A or 10A, as heretofore changed, remains unchanged and in full force and effect.

15A. NAME AND TITLE OF SIGNER *(Type or print)*		16A. NAME AND TITLE OF CONTRACTING OFFICER *(Type or print)*	
15B. CONTRACTOR/OFFEROR *(Signature of person authorized to sign)*	15C. DATE SIGNED	16B. UNITED STATES OF AMERICA *(Signature of Contracting Officer)*	16C. DATE SIGNED

Emergent IV BAA0001-22, dated June 14, 2022, is hereby Amended as follows:

The purpose of this modification is to answer questions relating to Hackathon and revise the date of demonstrations.

1. The purpose of this modification is to answer questions relating to Hackathon.

    a. **Question:** First, in the updated Q&A, a SITREP use case was discussed. Is it possible to get access to this use case?

    No, the use case is only provided if a full Cost and Technical Proposal is requested.

    b. **Question:** Second, I also saw in the Q&As that the effort would use data designated as "unclassified/CUI and higher". Do companies need to have cleared personnel to work on the hackathon?

    No.

    c. **Question:** Please confirm that we can include a Table of Contents and Table of Exhibits outside of the 20 page maximum count for the Technical volume?

    Per page 10 of the Emergent IV BAA, Resumes and certifications for technical data and computer software are the only documents that will not be counted as part of the 20-page limit. Additionally, page 10 states “No more than twenty (20) single-sided pages including, body, appendices, and attachments.”

    d. **Question:** Regarding the past performance requirements from Emergent IV BAA Section E.13.a, would the government consider changing the past performance requirement to "up to 5" rather than "five (5) accounts/contracts/projects"? Given the 20 page limit for all requirements, requiring 5 project writeups limits the page count to address all of the other technical requirements.

    No, this is an Emergent IV BAA requirement.

    e. **Question:** Regarding the proposal instructions from Emergent IV BAA Section D, would the government please exclude the past performance from the page count to allow adequate page count to cover all other technical proposal contents?

    No, this is an Emergent IV BAA requirement.

f. **Question:** Would the government please provide Small Business Subcontracting goals?

The FY2023 goals can be found here:
https://business.defense.gov/About/Goals-and-Performance/
Effective immediately, the SDVOSB subcontracting goal was recently increased to 5% from 3%.

g. **Question:** Please confirm that the Technical Proposal for the Hackathon, Emergent IV BAA, is for the Phase 1 as defined in Section 2.0 of the Statement of Work (SOW).

No, the technical and cost proposal are related to all three phases and should reflect your technical and functional approaches to address each areas of those phases in totality.

h. **Question:** Section F.1 – Cost Proposal Format of the Emergent IV BAA (pg. 16) states that "Respondents shall submit cost proposals within 30 calendar days of contracting officer's request…" However, per Amendment 21, the deadline for all selectees to submit their full technical and cost Proposals is Wednesday, May 22, 2024, and therefore over 30 days from when the contracting officer requested the technical and cost proposals (April 3, 2024). Due to this, can DLA confirm that the 30 calendar days requirement is no longer valid?

For Hackathon only, vendors should adhere to the timeline in Amendment 21.

i. **Question:** Can DLA confirm that it intends to provide DLA R&D Azure cloud environment or standalone GFE computers to a funded performer, and if so how many seats or laptops?

DLA is cloud agnostic. Therefore, the solution shall be able to operate on any cloud platform. DLA shall provide access to the cloud platforms as well government furnished equipment and materials to assist vendor development efforts.

j. **Question:** If selected for funded work, is the resulting contract(s) expected to include any additional terms (e.g. FAR/DFARS, etc.) not included in this BAA package that a performer must comply with?

Yes, the contract award document will include FAR, DFARS, and supplemental terms that are not included in the BAA that a performer must comply with.

k. **Question:** Can DLA provide a list of all the cyber security requirements and policies that a funded performer must comply with?

Laws, Regulations and DLA Cyber Regulation
The following laws and regulations apply to the information system:,

- Computer Fraud and Abuse Act [PL 99-474, 18 USC 1030]
- E-Authentication Guidance for Federal Agencies [OMB M-04-04]
- Federal Information Security Management Act (FISMA) of 2002 [Title III, PL 107-347]
- Freedom of Information Act As Amended in 2002 [PL 104-232, 5 USC 552]
- Guidance on Inter-Agency Sharing of Personal Data – Protecting Personal Privacy [OMB M-01-05]
- Homeland Security Presidential Directive-7, Critical Infrastructure Identification, Prioritization, and Protection [HSPD-7]
- Internal Control Systems [OMB Circular A-123]
- Management of Federal Information Resources [OMB Circular A-130]
- Management's Responsibility for Internal Control [OMB Circular A-123, Revised 12/21/2004]
- Privacy Act of 1974 as amended [5 USC 552a]
- Protection of Sensitive Agency Information [OMB M-06-16]
- Records Management by Federal Agencies [44 USC 31]
- Responsibilities for the Maintenance of Records About Individuals by Federal Agencies [OMB Circular A-108, as amended]
- Security of Federal Automated Information Systems [OMB Circular A-130, Appendix III]
- Federal Information Security Management Act of 2002, Title III – Information Security, P.L. 107-347.
- Consolidated Appropriations Act of 2005, Section 522.
- USA PATRIOT Act (P.L. 107-56), October 2001.
- OMB Circulars:
- OMB Circular A-130, Management of Federal Information Resources, November 2000.
- OMB Memorandum M-05-24, Implementation of Homeland Security Presidential Directive (HSPD) 12—Policy for a Common Identification Standard for Federal Employees and Contractors, August 2005.
- OMB Memorandum M-06-16, Protection of Sensitive Agency Information, June 2006.
- FIPS Publications:
- FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004

- FIPS PUB 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006
- FIPS PUB 201-2, Personal Identity Verification (PIV) of Federal Employees and Contractors, August 2013
- NIST Publications:
- NIST Special Publication (SP) 800-18 Rev1, Guide for Developing Security Plans for Information Technology Systems, February 2006
- NIST SP 800-21 2nd Edition, Guideline for Implementing Cryptography in the Federal Government, December 2005
- NIST SP 800-30 Rev1, Risk Management Guide for Information Technology Systems, September 2012
- NIST SP 800-34 Rev1, Contingency Planning Guide for Information Technology Systems, May 2010 (including updates as of 11 November 2010)
- NIST SP 800-37 Rev1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, February 2010 (includes updates as of 5 June 2014)
- NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems
- NIST SP 800-53 Rev4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013
- NIST SP 800-53A Rev1, Guide for Assessing the Security Controls in Federal Information System and Organizations, June 2010
- NIST SP 800-60 Rev1, Guide for Mapping Types of Information and Information Systems to Security, August 2008
- NIST SP 800-63-2, Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology, August 2013
- NIST SP 800-64 Rev2, Security Considerations in the Information System Development Life Cycle, October 2008

Department of Defense (DoD) Issuances:

- DoD Instruction (DoDI) 8510.01, Risk Management Framework (RMF) for DOD Information Technology (IT), 12 March 2014
- Committee on National Security Systems Instruction (CNSSI) 1253 Version 2, Security Categorization and Control Selection for National Security Systems, 15 March 2012
- DoDI 5200.48 Controlled Unclassified Information (CUI)
- DLAI 5200.48 Controlled Unclassified Information (CUI)
- DoD CUI Registry https://dlamil.dps.mil/sites/Intelligence/cui
- Information Officer Memorandum, “Control Systems Cybersecurity,” December 18, 2018
- Addendum - FRCS Master List Final_20201115

ARTET Documentation & Artifacts (Templates Available upon Request)

Automated Information Systems Inventory Spreadsheet (AISIS) Request Form:

- a complete initial inventory of your system organized in nine tabs representing specific details of your system.

Information Technology Solutions Document (ITSD) Management Approval:

- The ITSD serves as an auditable enforcement document to set parameters for managing the solutions that may be installed on the DLA network, and to outline any caveats that may limit Enterprise-wide use of listed solutions. The intent is to maintain solutions on the ITSD that are authorized, current, verifiable, vendor supported, licensed, compliant, sponsored, and funded (except for freeware). Reference DLAI 8210.01

Cybersecurity Questionnaire (CSQ):

- Helps PM/SM and ISSMs outline the most effective cybersecurity strategies to meet Risk Management Framework security controls.

Hardware/Software Spreadsheet:

- Essential for enabling application whitelisting/blacklisting and network access controls by identifying present hardware and software.

Ports, Protocols, and Services Management (PPSM) Spreadsheet*:

- Aligns with DoD Instruction 8551.01 to standardize the management of Internet protocol suite components, crucial for protecting DoD operations. Enterprise Connections PPSM – DoD Cyber Exchange

FIPS 199 System Categorization:

- Guides Federal agencies in assessing their systems' impact levels in terms of confidentiality, integrity, and availability. The scope of the FIPS-199 Categorization template includes the assessment of the information type categories as defined in the NIST Special Publication (SP) 800-60 Volume 2 Revision 1 document. FRCS system categorization is further defined in the FRCS Master List provided as addendum to the Chief Information Officer Memorandum, "Control Systems Cybersecurity," December 18, 2018.

Lean Cybersecurity Risk Assessment (LCRA) Application CONOP:

- to a system security plan, provides a security-focused system overview, including operational policies and user interactions.

Basic Cybersecurity Assessment (BCSA) Checklist for Server/Virtual:

- Necessary for documenting the cybersecurity posture of **each** server (Application, Database, etc.).

Architecture Diagram*:

- Illustrates the physical setup of application components, showcasing the structure, connections, and boundaries.

Dataflow Diagram*:

- Details the information flow within any process or system.

Dictionary for ARTET Applications:

- A comprehensive collection of data dictionary entries for easy lookup by entity identifier.

Required Application Scans and Security Technical Implementation Guides (STIGs):

- Compliance with STIGs and application scanning (e.g., ACAS, IVAM Compliance, Web Inspect) is **mandatory** for securing DoD IT networks and systems.
- Official DISA STIG Site: Security Technical Implementation Guides (STIGs) – DoD Cyber Exchange

Minimum Security Controls

- Security controls must meet minimum security control baseline requirements. There are security control baseline requirements for management controls, operational controls, and technical controls.

l. **Question:** If selected for funded work, will DLA include all three project phases (SOW 2.0) in a single award or will DLA request additional proposals for each of these project phases?

All three project phases shall be included in a single award. No additional proposal will be requested.

m. **Question:** Seeing that Amendment 19 and 20 answer questions regarding the use case for Hackathon. It is clear that the use case is focused on SITREPs. After looking through all the amendments, it is still unclear to me where the SITREP use case is defined by DLA outside of the Q&A amendments (19& 20). Would you be able to provide any guidance on where DLA originally defined the SITREP use case (document/section/page number) outside the Q&A?

You would not have received it because the Government did not request a full cost and technical proposal from your firm. The use case is sent out only if a proposal is requested.

n. **Question:** I imagine that if the white paper is being reopened there is a possibility that additional cost and technical proposals will be requested from additional vendors?

Correct.

o. **Question:** Could you provide a detailed breakdown of the expected costs associated with the Proof of Concept (POC)?

The Government expects the vendor to provide the breakdown of costs per the guidance in the BAA to support functional and technical requirements.

p. **Question:** How will changes to the project backlog affect the cost and schedule?

DLA does not have or is expecting a backlog for this project. Therefore, with no project backlog there should not be a cost/schedule or performance, risk or issues.

q. **Question:** How do you anticipate changes to the project backlog to affect cost and schedule post-POC?

As stated in the previous question, DLA is not anticipated any changes to a proceed project backlog that could potentially effect pre or post POC.

r. **Question:** Can you specify the expected range of users for the POC?

DLA has the potential to onboard over 25K employees across CONOS and OCONUS locations; however, DLA plans to take a phase-by-phase approach to implementing the capability.

s. **Question:** How do you anticipate the number of users to scale post-POC?

Based on the solutions implemented it will be available to use across the DLA enterprise. It should consider helpdesk and other technical functional workforce requirements to the various user community within DLA to scale during implementation phases.

t. **Question:** What are the estimated volumes and velocity of data ingestion and processing?

Based on the Use Case requirements, DLA is leveraging our existing data ingestion and processing to determine volume and velocity to support the project implementation.

u. **Question:** Could you describe the data lifecycle management policies that will be in place?

DLA will leverage their data based on our current practices with OSD, ADVANA, and the Services' data on management policies. Moreover, based on DLA requirements, we will develop ongoing management policies to address our specific data needs.

v. **Question:** Will the system need to handle multimodal data (e.g., text, images, audio)?

Yes, DLA is highly interested in vendors providing various multi model data sources (standard and non-standard) to train their models to support DLA mission sets.

w. **Question:** Are there any specific data formats or standards that the system should comply with?

DLA requires DoD sanction data formats standards to include, but not limited to, JSON, XML, CSV, PNG, JPEG, MP3, MP4.

x. **Question:** What are the specific output formats required for the product (e.g., JSON, XML, CSV)?

Please see response above that has specific output formats that compile with DLA, DoD, and industry standards. Please note DLA is also interested in non-traditional formats to further develop our data pool.

y. **Question:** How should the system handle report generation and data visualization?

DLA has a library of report generation and data visualization tools to include QLIK, ServiceNow, PowerBI, SAS, etc., with an expectation that the vendor will be able to leverage the existing tools as well as provide additional sources approved by DoD software requirements.

z. **Question:** Will the users be centrally located or geographically distributed?

DLA workforce consist of users located CONUS and OCUNUS, please referred to the DLA webpage (www.dla.mil) for additional geographic information.

aa. **Question:** Are there any user role-based access controls or customization requirements?

Based on the vendors approved credentials they will be able to access the enterprise-wide capabilities. Additionally, there is no customization requirements needed.

bb. **Question:** What are the performance metrics or KPIs that will be used to evaluate the success of the POC?

DLA will evaluate the success of the POC based on current Supply Chain Risk Management (SCRM)'s methodology and approach for the supply chain.

cc. **Question:** Can you provide examples of use cases or user stories that the POC should address?

The use case will be provided only if a full Cost and Technical Proposal is requested.

dd. **Question:** What are the integration requirements with existing systems or data sources?

DLA is a cloud agnostic environment with interoperability with our ServiceNow platform with API sanction by other enterprise tooling to include LINUX, Microsoft, Oracle, SAP, SAS, QLIK, Python, etc. This list is just a sample of enterprise integration tools and not an entire representation, the intent is for the vendor provide their integration capabilities.

ee. **Question:** Amendment 21 revised the overall timeline, stating "The Contracting Officer will notify new selectees to submit full Technical and Cost Proposals." Can the government confirm that all of the original selectees are moving forward to submit full Technical and Cost Proposals?

Correct.

ff. **Question:** Is the White Paper due by 5pm EST Friday, 26 April or 11:59pm EST Friday, 26 April?

11:59 PM EST on Friday, April 26, 2024

gg. **Question:** For the White Paper Cover Sheet and the White Paper Project Summary template, is it expected that the requested information (Project Title; Proposer Organization; Technical POC; Administrative POC; Other Team Members; Estimated Total Cost; Estimated PoP; and Other Solicitations) is copied? If so, can a responder simply fill out the White Paper Cover Sheet and use the Project Summary page limit (4 pgs.) to solely address the SOW/4.0 Scope and not repeat the tabled information?

The vendor is required to submit a White Paper that adheres to the requirements of Attachment C: White Paper Template starting on page 28 of the Emergent IV BAA.

hh. **Question:** For the White Paper Cover Sheet, can the responder select more than one BAA Area of Interest from Attachment B?

Hackathon is based on AOI H, Artificial Intelligence / Machine Learning (AI/ML) application as identified in the SOW in Amendment 21.

ii. **Question:** For the White Paper Project Summary, please confirm that the responder only has to respond to one of the areas from the SOW, Scope 4.0, 1.-14.

Correct, per section 4.0 Scope on page 6 of Amendment 21, "The vendor will select specific **area(s)** from the listing below to respond to the SOW via the White Paper (WP) submission"

jj. **Question**: Is NIST 800-171 compliance required to Prime?"

Complying with NIST 800-171 is required for any non-federal organization that handles CUI. This includes Prime contractors working for the DoD and their subcontractors, as well as universities and research institutions receiving federal grants. Compliance determines whether these organizations are eligible to do business with the DoD and reap the rewards of the associated federal funds.

2. The date of In-person Demonstrations is hereby revised from Wednesday, June 27, 2024 to **Monday, June 24, 2024.**

3. All other Terms and Conditions remain unchanged.