

AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT		1. CONTRACT ID CODE		PAGE OF PAGES 1 2	
2. AMENDMENT/MODIFICATION NO. 0151		3. EFFECTIVE DATE See Block 16C		4. REQUISITION/PURCHASE REQ. NO.	
6. ISSUED BY NNSA M&O Contracting Branch NA-APM-131 Albuquerque Complex P.O. Box 5400 Albuquerque NM 87185-5400		CODE 892332		5. PROJECT NO. (If applicable) 7. ADMINISTERED BY (If other than Item 6) NNSA Nevada Field OFC NA-00-NV P.O. Box 98518 Las Vegas NV 89193-8518	
8. NAME AND ADDRESS OF CONTRACTOR (No., street, county, State and ZIP Code) Mission Support And Test Services LLC Attn: Paul Spickard PO Box 98521 M/S NLV019 Las Vegas NV 891938421		(x)		9A. AMENDMENT OF SOLICITATION NO.	
CODE 080083514		FACILITY CODE		9B. DATED (SEE ITEM 11)	
		X		10A. MODIFICATION OF CONTRACT/ORDER NO. DE-NA0003624	
				10B. DATED (SEE ITEM 13) 05/12/2017	

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 electronic communication which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGEMENT 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 you desire to change an offer already submitted, such change may be made by letter or electronic communication, provided each letter or electronic communication makes reference to the solicitation and this amendment, and is received prior to the opening hour and date specified.

12. ACCOUNTING AND APPROPRIATION 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 data, 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:
X	D. OTHER (Specify type of modification and authority) DEAR 970.5204-2, Laws, Regs & DOE Directives & Agreement of Parties

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.)

UEI: YSYZHPG4XB3

The purpose of this modification is to update clauses in Section I, revise/update directives in Appendix F, revise the Compensation Section of Appendix G, and update the Key Personnel list in Appendix H as set for in Attachment 1.

Continued ...

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

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

Previous edition unusable

NAME OF OFFEROR OR CONTRACTOR
Mission Support And Test Services LLC

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	Payment: Period of Performance: 06/07/2017 to 11/30/2022				

I. PART II – Contract Clauses, SECTION I – Contract Clauses, is modified as follows:

- a. The Table of contents is modified by updating the date of the clauses as set forth in the table below.**

Clause No.	Clause Title/Date
I-1A	FAR 52.204-21 BASIC SAFEGUARDING OF COVERED CONTRACTOR INFORMATION SYSTEMS (Nov 2021)
I-1B	FAR 52.204-25 PROHIBITION ON CONTRACTING FOR CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT (Nov 2021)
I-24	FAR 52.204-23 PROHIBITION ON CONTRACTING FOR HARDWARE, SOFTWARE, AND SERVICES DEVELOPED OR PROVIDED BY KASPERSKY LAB AND OTHER COVERED ENTITIES (NOV 2021)

- b. PARAGRAPH C. – FAR AND DEAR CLAUSES INCORPORATED IN FULL TEXT, is modified as follows:**

- i. Delete Clause I-1A, FAR 52.204-21 – BASIC SAFEGUARDING OF COVERED CONTRACTOR INFORMATION SYSTEMS (JUN 2016), in its entirety and replace with the text set forth below.**

I-1A FAR 52.204-21 BASIC SAFEGUARDING OF COVERED CONTRACTOR INFORMATION SYSTEMS (Nov 2021)

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

Covered contractor information system means an information system that is owned or operated by a contractor that processes, stores, or transmits Federal contract information.

Federal contract information means information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as on public websites) or simple transactional information, such as necessary to process payments.

Information means any communication or representation of knowledge such as facts, data, or opinions, in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual (Committee on National Security Systems Instruction (CNSSI) 4009).

Information system means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (44 U.S.C. 3502).

Safeguarding means measures or controls that are prescribed to protect information systems.

- (b) Safeguarding requirements and procedures.

- (1) The Contractor shall apply the following basic safeguarding requirements and procedures to protect covered contractor information systems. Requirements and procedures for basic safeguarding of covered contractor information systems shall include, at a minimum, the following security controls:
 - (i) Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).
 - (ii) Limit information system access to the types of transactions and functions that authorized users are permitted to execute.
 - (iii) Verify and control/limit connections to and use of external information systems.
 - (iv) Control information posted or processed on publicly accessible information systems.
 - (v) Identify information system users, processes acting on behalf of users, or devices.
 - (vi) Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.
 - (vii) Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.
 - (viii) Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.
 - (ix) Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.
 - (x) Monitor, control, and protect organizational communications (*i.e.*, information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.
 - (xi) Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.
 - (xii) Identify, report, and correct information and information system flaws in a timely manner.
 - (xiii) Provide protection from malicious code at appropriate locations within organizational information systems.
 - (xiv) Update malicious code protection mechanisms when new releases are available.
 - (xv) Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.
- (2) *Other requirements.* This clause does not relieve the Contractor of any other specific safeguarding requirements specified by Federal agencies and departments relating to covered

contractor information systems generally or other Federal safeguarding requirements for controlled unclassified information (CUI) as established by Executive Order 13556.

- (c) *Subcontracts.* The Contractor shall include the substance of this clause, including this paragraph (c), in subcontracts under this contract (including subcontracts for the acquisition of commercial products or commercial services, other than commercially available off-the-shelf items), in which the subcontractor may have Federal contract information residing in or transiting through its information system.

(End of clause)

ii. Delete Clause I-1B, FAR 52.204-25 – PROHIBITION ON CONTRACTING FOR CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT (AUG 2020), in its entirety and replace with the text set forth below.

I-1B FAR 52.204-25 PROHIBITION ON CONTRACTING FOR CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT (NOV 2021)

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

Backhaul means intermediate links between the core network, or backbone network, and the small subnetworks at the edge of the network (e.g., connecting cell phones/towers to the core telephone network). Backhaul can be wireless (e.g., microwave) or wired (e.g., fiber optic, coaxial cable, Ethernet).

Covered foreign country means The People's Republic of China.

- (1) Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities);
- (2) For the purpose of public safety, security of Government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities);
- (3) Telecommunications or video surveillance services provided by such entities or using such equipment; or
- (4) Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country.

Critical technology means—

- (1) Defense articles or defense services included on the United States Munitions List set forth in the International Traffic in Arms Regulations under subchapter M of chapter I of title 22, Code of Federal Regulations;

- (2) Items included on the Commerce Control List set forth in Supplement No. 1 to part 774 of the Export Administration Regulations under subchapter C of chapter VII of title 15, Code of Federal Regulations, and controlled-
 - (i) Pursuant to multilateral regimes, including for reasons relating to national security, chemical and biological weapons proliferation, nuclear nonproliferation, or missile technology; or
 - (ii) For reasons relating to regional stability or surreptitious listening
- (3) Specially designed and prepared nuclear equipment, parts and components, materials, software, and technology covered by part 810 of title 10, Code of Federal Regulations (relating to assistance to foreign atomic energy activities);
- (4) Nuclear facilities, equipment, and material covered by part 110 of title 10, Code of Federal Regulations (relating to export and import of nuclear equipment and material);
- (5) Select agents and toxins covered by part 331 of title 7, Code of Federal Regulations, part 121 of title 9 of such Code, or part 73 of title 42 of such Code; or
- (6) Emerging and foundational technologies controlled pursuant to section 1758 of the Export Control Reform Act of 2018 (50 U.S.C. 4817).

Interconnection arrangements means arrangements governing the physical connection of two or more networks to allow the use of another's network to hand off traffic where it is ultimately delivered (e.g., connection of a customer of telephone provider A to a customer of telephone company B) or sharing data and other information resources.

Reasonable inquiry means an inquiry designed to uncover any information in the entity's possession about the identity of the producer or provider of covered telecommunications equipment or services used by the entity that excludes the need to include an internal or third-party audit.

Roaming means cellular communications services (e.g., voice, video, data) received from a visited network when unable to connect to the facilities of the home network either because signal coverage is too weak or because traffic is too high.

Substantial or essential component means any component necessary for the proper function or performance of a piece of equipment, system, or service.

(b) *Prohibition.*

- (1) Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2019, from procuring or obtaining, or extending or renewing a contract to procure or obtain, any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. The Contractor is prohibited from providing to the Government any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an

exception at paragraph (c) of this clause applies or the covered telecommunication equipment or services are covered by a waiver described in FAR [4.2104](#).

- (2) Section 889(a)(1)(B) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2020, from entering into a contract, or extending or renewing a contract, with an entity that uses any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception at paragraph (c) of this clause applies or the covered telecommunication equipment or services are covered by a waiver described in FAR [4.2104](#). This prohibition applies to the use of covered telecommunications equipment or services, regardless of whether that use is in performance of work under a Federal contract.

(c) *Exceptions.* This clause does not prohibit contractors from providing—

- (1) A service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or
- (2) Telecommunications equipment that cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(d) *Reporting requirement.*

- (1) In the event the Contractor identifies covered telecommunications equipment or services used as a substantial or essential component of any system, or as critical technology as part of any system, during contract performance, or the Contractor is notified of such by a subcontractor at any tier or by any other source, the Contractor shall report the information in paragraph (d)(2) of this clause to the Contracting Officer, unless elsewhere in this contract are established procedures for reporting the information; in the case of the Department of Defense, the Contractor shall report to the website at <https://dibnet.dod.mil>. For indefinite delivery contracts, the Contractor shall report to the Contracting Officer for the indefinite delivery contract and the Contracting Officer(s) for any affected order or, in the case of the Department of Defense, identify both the indefinite delivery contract and any affected orders in the report provided at <https://dibnet.dod.mil>.
- (2) The Contractor shall report the following information pursuant to paragraph (d)(1) of this clause
 - (i) Within one business day from the date of such identification or notification: the contract number; the order number(s), if applicable; supplier name; supplier unique entity identifier (if known); supplier Commercial and Government Entity (CAGE) code (if known); brand; model number (original equipment manufacturer number, manufacturer part number, or wholesaler number); item description; and any readily available information about mitigation actions undertaken or recommended.
 - (ii) Within 10 business days of submitting the information in paragraph (d)(2)(i) of this clause: any further available information about mitigation actions undertaken or recommended. In addition, the Contractor shall describe the efforts it undertook to prevent use or submission of covered telecommunications equipment or services, and any additional efforts that will be incorporated to prevent future use or submission of covered telecommunications equipment or services.

- (c) *Subcontracts.* The Contractor shall insert the substance of this clause, including this paragraph (c) and excluding paragraph (b)(2), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial products or commercial services.

(End of clause)

iii. Delete Clause I-24, FAR 52.204-23 – PROHIBITION ON CONTRACTING FOR HARDWARE, SOFTWARE, AND SERVICES DEVELOPED OR PROVIDED BY KASPERSKY LAB AND OTHER COVERED ENTITIES (JUL 2018), in its entirety and replace with the text set forth below.

I-24 FAR 52.204-23 PROHIBITION ON CONTRACTING FOR HARDWARE, SOFTWARE, AND SERVICES DEVELOPED OR PROVIDED BY KASPERSKY LAB AND OTHER COVERED ENTITIES (NOV 2021)

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

Covered article means any hardware, software, or service that—

- (1) *Is developed or provided by a covered entity;*
- (2) *Includes any hardware, software, or service developed or provided in whole or in part by a covered entity; or*

Covered entity means—

- (1) *Kaspersky Lab;*
- (2) *Any successor entity to Kaspersky Lab;*
- (3) *Any entity that controls, is controlled by, or is under common control with Kaspersky Lab; or*
- (4) *Any entity of which Kaspersky Lab has a majority ownership.*

- (b) *Prohibition.* Section 1634 of Division A of the National Defense Authorization Act for Fiscal Year 2018 (Pub. L. 115-91) prohibits Government use of any covered article. The Contractor is prohibited from—

- (1) Providing any covered article that the Government will use on or after October 1, 2018; and
- (2) Using any covered article on or after October 1, 2018, in the development of data or deliverables first produced in the performance of the contract.

- (c) *Reporting requirement.*

- (1) In the event the Contractor identifies a covered article provided to the Government during contract performance, or the Contractor is notified of such by a subcontractor at any tier or any other source, the Contractor shall report, in writing, to the Contracting Officer or, in the case of the Department of Defense, to the website at <https://dibnet.dod.mil>. For indefinite delivery contracts,

the Contractor shall report to the Contracting Officer for the indefinite delivery contract and the Contracting Officer(s) for any affected order or, in the case of the Department of Defense, identify both the indefinite delivery contract and any affected orders in the report provided at <https://dibnet.dod.mil>.

(2) The Contractor shall report the following information pursuant to paragraph (c)(1) of this clause:

- (i) Within 1 business day from the date of such identification or notification: the contract number; the order number(s), if applicable; supplier name; brand; model number (Original Equipment Manufacturer (OEM) number, manufacturer part number, or wholesaler number); item description; and any readily available information about mitigation actions undertaken or recommended.
- (ii) Within 10 business days of submitting the report pursuant to paragraph (c)(1) of this clause: any further available information about mitigation actions undertaken or recommended. In addition, the Contractor shall describe the efforts it undertook to prevent use or submission of a covered article, any reasons that led to the use or submission of the covered article, and any additional efforts that will be incorporated to prevent future use or submission of covered articles.
- (d) Subcontracts. The Contractor shall insert the substance of this clause, including this paragraph (d), in all subcontracts including subcontracts for the acquisition of commercial products or commercial services.

(End of clause)

II. PART III – LIST OF DOCUMENTS, EXHIBITS, AND OTHER ATTACHMENTS, SECTION J – LIST OF ATTACHMENTS, is modified as set forth below.

a. APPENDIX F – List of Applicable Laws, Regulations, and DOE Directives is modified as follows:

i. Add the following entry:

DIRECTIVE NUMBER			DATE	DOE DIRECTIVE TITLE
NNSA	SD	452-4.1	1-27-2022	Nuclear Enterprise Assurance (NEA)

ii. Update the “Directive Number” and “Date” for the directives set forth in the table below.

DIRECTIVE NUMBER			DATE	DOE DIRECTIVE TITLE	MOD #
NAP		401.1A Admin Chg 2	2/15/2022	Weapons Quality Policy	0151
DOE	O	472.2A	6/10/2022	Personnel Security	0151

- b. **Appendix G – Personnel Appendix, Paragraph 3.0, Compensation, is modified by deleting the table under subparagraph 3.2 – Overtime, 3. Exempt Employees, and inserting the table set forth below. This table expands the job groups and levels that may be paid overtime as described in the paragraph.**

JOB GROUP	LEVEL(S)	JOB GROUP	LEVEL(S)
Management	I, II	Project & Business Management	I,II,III (Mod 0076)
Scientists & Engineers	I, II, III, IV	Technical Support	VI
Technical Professionals	II, III, IV	IT Professionals	III, IV
Business Professionals	II, III, IV	Technical Management	I, II

- c. **Appendix H – Key Personnel is modified by deleting the existing table and inserting the table below. This table removes the name cited as the Senior Director, Stockpile Experimentation and Operations (SEO) position.**

Name	Position
Mark W. Martinez	President
Roger R. Rocha	Vice President & Chief Operating Officer, Mission Operations
TBD	Senior Director, Stockpile Experimentation and Operations (SEO)
TBD	Senior Director, Infrastructure
John S. Contardi	Senior Director, Mission Assurance
Neile Miller	Senior Director, Business Operations
Mark J. Krauss	Senior Director, Stockpile Operations & Environmental Management Program
Craig R. Wuest	Senior Director, Mission Development, Senior Intelligence Executive; Field Intelligence Element
Darcie Dennis-Koller	Senior Director, Global Security

No further changes are made as a result of this modification.

END OF MODIFICATION