EXCEPTION TO SF 30, APPROVED BY NARS 5/79

AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT

1. CONTRACT ID CODE | PAGE 1 OF 7

2. AMENDMENT/MODIFICATION NO.	3. EFFECTIVE DATE	4. REQUISITION/PURCHASE REQ. NO.	5. PROJECT NO. *(If applicable)*
908	See block 16 c.	**NA27344**	

6. ISSUED BY CODE	7. ADMINISTERED BY *(If other than Item 6)* CODE
U.S. Department of Energy/NNSA SC M&O Contract Support Division P.O. Box 5400 Albuquerque, NM 87185-5400	U.S. Department of Energy/NNSA Livermore Site Office M/S L-293 7000 East Avenue Livermore, CA 94550

8. NAME AND ADDRESS OF CONTRACTOR *(No., street, country, State, and ZIP Code)*		9A. AMENDMENT OF SOLICITATION NO.
Lawrence Livermore National Security, LLC Lawrence Livermore National Laboratory M/S L-019 7000 East Avenue Livermore, CA 94550		
		9B. DATED *(SEE ITEM 11)*
	X	10A. MODIFICATION OF CONTRACT/ ORDER NO. DE-AC52-07NA27344
		10B. DATED *(SEE ITEM 13)*
CODE / FACILITY CODE		May 8, 2007

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 25, 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 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 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 APPROPRIATION DATA *(If required)*

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

	A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: *(Specify authority)* THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN 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).
X	C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF: Clause H-19 Modification Authority, Clause I-120 Changes, and Mutual Agreement
	D. OTHER *(Specify type of modification and authority)*

E. IMPORTANT: Contractor __ is not, _X_ is required to sign this document and return _1_ copies to the issuing office.

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

See page 2.

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)*
Joseph (Trey) Johnston Lawrence Livermore National Security, LLC	Inderpreet Chahal, Contracting Officer U.S. Department of Energy/NNSA

15B. CONTRACTOR/OFFEROR	15C. DATE SIGNED	16B. UNITED STATES OF AMERICA	16C. DATE SIGNED
Joseph E. Johnston Digitally signed by Joseph E. Johnston Date: 2025.10.17 17:46:02 -07'00' *(Signature of person authorized to sign)*		INDERPREET CHAHAL Digitally signed by INDERPREET CHAHAL Date: 2025.10.17 19:08:15 -07'00' By *(Signature of Contracting Officer)*	

A. PURPOSE:

The purpose of this modification is to Update Part III, Section J, Appendix G DOE O 414.1E; Update Part I, Section B, Clause B-2(f)(2)(i)(I) monthly provisional fee payments from 3% to 6%; Add clause H-60: Safeguarding Covered NNSA Information, Cloud Computing Services, And Cybersecurity Incident Reporting to Part I, Section H.

B. CHANGES TO THE CONTRACT

As the result of this modification, the following changes are hereby incorporated into the Contract:

1. Part III, Section J, Appendix G, DOE O 414.1E has been updated to reflect that an Implementation Plan is included.

2. Part I, Section B, Clause B-2(f)(2)(i)(I) monthly provisional fee payments has been updated from:

(I) in monthly provisional fee payments equivalent to 3% of the Maximum Available Performance Incentive Fee, and

to:

(I) in monthly provisional fee payments equivalent to 6% of the Maximum Available Performance Incentive Fee, and

3. The following clause has been added to Part I, Section H:

H-60 SAFEGUARDING COVERED NNSA INFORMATION, CLOUD COMPUTING SERVICES, AND CYBERSECURITY INCIDENT REPORTING (JUL 2025) (Mod XXX)

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

"Authorizing official," as defined by the National Institute of Standards and Technology (NIST) (https://csrc.nist.gov/glossary/term/authorizing_official), means the senior Federal official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

"Cloud computing," as used in this provision, means a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This includes other commercial terms, such as on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. It also includes commercial offerings for software-as-a-service, infrastructure-as-a-service, and platform-as-a-service.

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

"Contractor/corporate-owned records" means records not identified as Federal records (such as company proprietary information, records unrelated to the work performed under a federal contract, and other similar records) that belong to the contractor. Contractor/corporate-owned records are defined in the contract and/or through the Access to an Ownership of Records clause (48 CFR 970.5204.3). Privacy Act Systems of Record [Federal Acquisition Regulation (FAR) 52-224-2] are NOT contractor-owned records.

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

"Covered NNSA Information" means unclassified controlled technical information or other information, as described in the Controlled Unclassified Information (CUI) Registry at https://www.archives.gov/cui/registry/category-list.html, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, Department of Energy Order 471.7, and Governmentwide policies, and is—

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

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

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

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

"Government data" means any information, document, media, or machine-readable material regardless of physical form or characteristics, that is created or obtained by the Government in the course of official Government business.

"Government-related data" means any information, document, media, or machine-readable material regardless of physical form or characteristics that is created or obtained by a contractor through the storage, processing, or communication of Government data. This does not include contractor's business records (e.g., financial records, legal records, etc.) or data such as operating procedures, software coding or algorithms that are not uniquely applied to the Government data.

"Information technology" has the meaning assigned in section 11101 of title 40, including cloud computing services of all types.

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

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

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

"Spillage" security incident that results in the transfer of classified or controlled unclassified information onto an information system not accredited (i.e., authorized) for the appropriate security level.

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

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

(i) Cloud computing services shall be subject to the security requirements delineated in paragraphs (m) through (v).

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

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

(i) Except as provided in paragraph (b)(2)(ii) of this clause, the Contractor shall ensure that all covered contractor information systems comply with the security requirements identified in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" (available via the internet at https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final) in effect at the time the solicitation is issued or as authorized by the Contracting Officer.

(ii)(A) The Contractor shall implement the security requirements identified in NIST SP 800-171, as soon as practicable, but not later than twelve months after award; all software updates and patches shall be installed as soon as practicable or as applicable based on dependent application updates.

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

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

(c) *Cybersecurity incident reporting requirement.*

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

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

(ii) Report Cybersecurity incidents to the NNSA Information Assurance Response Center (IARC) in accordance with the IARC Cybersecurity Incident Reporting Standard Operating Procedure (IARC-SOP-24601) which can be requested from the IARC at iarc@nnsa.doe.gov.

(2) *Cybersecurity incident report*. The cybersecurity incident report shall be treated as covered NNSA information created by or for the IARC.

(d) *Malicious software*. When the Contractor discovers and isolates malicious software in connection with a reported cybersecurity incident, the Contractor shall submit the malicious software to the IARC in accordance with instructions provided by IARC or the Contracting Officer. Do not send the malicious software to the Contracting Officer.

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

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

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

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

(i) *Use and release of Contractor/corporate-owned records not created by or for NNSA.* Information that is obtained from the Contractor (or derived from information obtained from the Contractor) under this clause that is not created by or for NNSA is authorized to be released outside of NNSA—

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

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

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

(4) For national security purposes, including cybersecurity situational awareness; or

(5) To a support services contractor ("recipient") that is directly supporting Government activities under a contract in accordance with paragraph (w), *Limitations on the Use or Disclosure of Third-Party Contractor Reported Cybersecurity Incident Information*.

(j) *Use and release of Contractor attributional/proprietary information created by or for NNSA.* Information that is obtained from the Contractor (or derived from information obtained from the Contractor) under this clause that is created by or for NNSA (including the information submitted pursuant to paragraph (c) of this clause) is authorized to be used and released outside of NNSA for purposes and activities authorized by paragraph (i) of this clause, and for any other lawful Government purpose or activity, subject to all applicable statutory, regulatory, and policy based restrictions on the Government's use and release of such information.

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

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

(m) *Cloud computing security requirements*. The requirements of this paragraph (m) through (v) are applicable when using cloud computing to provide information technology services in the performance of the contract.

(1) The Contractor shall implement and maintain administrative, technical, and physical safeguards and controls in accordance with the latest versions of DOE Order 205.1 and NNSA SD 205.1, unless notified by the Contracting Officer that this requirement has been waived by the NNSA Chief Information Officer.

(2) The Contractor shall maintain all Government data that is not physically located on NNSA premises within the United States or outlying areas (as defined by 48 C.F.R. § 2.101), unless the Contractor receives written notification from the Contracting Officer to use another location.

(n) *Limitations on access to, and use and disclosure of Government data and Government-related data.*

(1) The Contractor shall not access, use, or disclose Government data unless specifically authorized by the terms of this contract or a task order or delivery order issued hereunder.

(i) If authorized by the terms of this contract or a task order or delivery order issued hereunder, any access to, or use or disclosure of, Government data shall only be for purposes specified in this contract or task order or delivery order.

(ii) The Contractor shall ensure that its employees are subject to all such access, use, and disclosure prohibitions and obligations.

(iii) These access, use, and disclosure prohibitions and obligations shall survive the expiration or termination of this contract.

(2) The Contractor shall use Government-related data only to manage the operational environment that supports the Government data and for no other purpose unless otherwise permitted with the prior written approval of the Contracting Officer.

(o) *Cloud computing services Cybersecurity incident reporting*. The Contractor shall report all Cybersecurity incidents that are related to the cloud computing service provided under this contract to the NNSA IARC in accordance with IARC Cybersecurity Incident Reporting Standard Operating Procedure (IARC-SOP-24601), which is available through contact with the IARC at iarc@nnsa.doe.gov.

(p) *Malicious software within the cloud computing environment*. The Contractor that discovers and isolates malicious software in connection with a reported Cybersecurity incident shall submit the malicious software to the IARC in accordance with instructions provided by IARC or the Contracting Officer. Do not send the malicious software to the Contracting Officer.

(q) *Media preservation and protection within the cloud computing environment*. When a Contractor discovers a Cybersecurity incident has occurred within the cloud computing environment, the Contractor shall preserve and protect images of all known affected information systems identified in the IARC Incident Reporting Form (see paragraph (o) of this clause) and all relevant monitoring/packet capture data for at least one year from the submission of the IARC Incident Reporting Form to allow NNSA to request the media.

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

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

(t) *Records management and facility access.*

(1) The Contractor shall provide the Contracting Officer all Government data and Government-related data in the format specified in the contract.

(2) The Contractor shall dispose of Government data and Government-related data in accordance with the terms of the contract and provide the confirmation of disposition to the Contracting Officer in accordance with contract closeout procedures.

(3) The Contractor shall provide the Government, or its authorized representatives, access to all Government data and Government-related data, access to Contractor personnel involved in performance of the contract, and physical access to any Contractor facility with Government data, for the purpose of audits, investigations, inspections, or other similar activities, as authorized by law or regulation.

(u*) Notification of third-party access requests*. The Contractor shall notify the Contracting Officer promptly of any requests from a third party for access to Government data or Government-related data, including any warrants, seizures, or subpoenas it receives, including those from another Federal, State, or local agency.

The Contractor shall cooperate with the Contracting Officer to take all measures to protect Government data and Government-related data from any unauthorized disclosure.

(v) *Spillage*. Upon notification by the Government of a spillage, or upon the Contractor's discovery of a spillage, the Contractor shall cooperate with the Contracting Officer to address the spillage in compliance with the IARC Cybersecurity Incident Reporting Standard Operating Procedure (IARC-SOP-24601), which is available through contact with the IARC at iarc@nnsa.doe.gov.

(w) *Limitations and restrictions on the use or disclosure of third-party contractor reported cybersecurity information*. The Contractor agrees that the following conditions apply to any information it receives or creates in the performance of this contract that is information obtained from a third-party's reporting of a Cybersecurity incident pursuant to paragraphs (c) through (l):

(1) The Contractor shall access and use the information only for the purpose of furnishing advice or technical assistance directly to the Government in support of the Government's activities related to paragraphs (c) through (l) and shall not be used for any other purpose.

(2) The Contractor shall protect the information against unauthorized release or disclosure.

(3) The Contractor shall ensure that its employees are subject to use and non-disclosure obligations consistent with this clause prior to the employees being provided access to or use of the information.

(4) Information provided by a third-party contractor reporting a Cybersecurity incident shall be subject to equivalent protection for use and non-disclosure obligations as those referred to in paragraph (w)(3) of this clause (with the exception that all information must be both useable and disclosable to the Government).

(5) A breach of these obligations or restrictions may subject the Contractor to criminal, civil, administrative, and contractual actions in law and equity for penalties, damages, and other appropriate remedies by the United States.

(x) *Subcontracts*. The Contractor shall—

(1) Include this clause, including paragraph (x), in subcontracts, or similar contractual instruments, for services that include support for the Government's activities related to safeguarding covered NNSA information, cloud services, and Cybersecurity incident reporting, including subcontracts for commercial products or commercial services, without alteration, except to identify the parties. The Contractor shall determine if the information required for subcontractor performance retains its identity as covered NNSA Information and will require protection under this clause, and, if necessary, consult with the Contracting Officer; and

(2) Require subcontractors to provide incident report information to the prime Contractor (or next higher-tier subcontractor) as soon as practicable, when reporting a cybersecurity incident to NNSA as required in paragraph (c) of this clause.

C. All other terms and conditions remain unchanged and in full force and effect.