AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT

1. CONTRACT ID CODE	PAGE OF PAGES
	1 16

2. AMENDMENT/MODIFICATION NO.	3. EFFECTIVE DATE	4. REQUISITION/PURCHASE REQ. NO.	5. PROJECT NO. *(If applicable)*
1117	See Block 16C		

6. ISSUED BY CODE 892332

NNSA M&O Contracting Branch
NA-PAS-211
Albuquerque Complex
P.O. Box 5400
Albuquerque NM 87185-5400

7. ADMINISTERED BY *(If other than Item 6)* CODE 05009

NNSA Savannah River Field OFC
NA-SV
P.O. Box A
Building 246-H
Aiken SC 29802

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

SAVANNAH RIVER NUCLEAR SOLUTIONS LLC
Attn: Keith Sawyer
203 LAURENS ST SW
AIKEN SC 298012421

CODE FACILITY CODE

(x) 9A. AMENDMENT OF SOLICITATION NO.

9B. DATED *(SEE ITEM 11)*

x 10A. MODIFICATION OF CONTRACT/ORDER NO. DE-AC09-08SR22470

10B. DATED *(SEE ITEM 13)* 01/10/2008

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)*
See Schedule

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).
X	C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF: FAR 43.103(a), Mutual Agreement of the Parties
	D. OTHER *(Specify type of modification and authority)*

E. IMPORTANT: Contractor ☐ is not ☒ 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.)*

The purpose of this modification is to revise the contract to implement changes associated with the contract transfer to NNSA as described in the SF30 Block 14 Continuation pages.

The contract estimated value and all other terms and conditions remain unchanged.
Payment:

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)*	16A. NAME AND TITLE OF CONTRACTING OFFICER *(Type or print)*
Richard Charles, Director Contracts	Cory L. Price

15B. CONTRACTOR/OFFEROR	15C. DATE SIGNED	16B. UNITED STATES OF AMERICA	16C. DATE SIGNED
[redacted] *(Signature of person authorized to sign)*	3/11/25	[redacted]	

SF30 Block 14 Continuation

A. Revise sentences in Part I, Section C, Paragraph C-1.1 to reflect the change in SRS landlord from Office of Environmental Management (EM) to National Nuclear Security Administration (NNSA) as follows:

A. From: DOE's Office of Environmental Management (EM) is the landlord for the SRS and responsible for cleanup missions and the Savannah River National Laboratory (SRNL).

To: DOE's Office of Environmental Management (EM) is ~~the landlord for the SRS and~~ responsible for cleanup missions and the Savannah River National Laboratory (SRNL).

B. From: The National Nuclear Security Administration (NNSA) is responsible for supporting the nuclear weapons stockpile programs and nonproliferation activities on the Site.

To: The National Nuclear Security Administration (NNSA) is *the landlord for the SRS effective October 1, 2024, and is* responsible for supporting the nuclear weapons stockpile programs and nonproliferation activities on the Site.

B. Part I, Section H, is revised to add clauses H-77 through H-84 as follows:

H-77 ACCOUNTABILITY

The Contractor is responsible for the quality of its products and services and for assessing its operations, programs, projects and business systems and identifying deficiencies and implementing needed improvements in accordance with the terms and conditions of this Contract, regardless of whether NNSA has evaluated the Contractor's performance in any area of the Contract. The Contractor is encouraged to collaborate with its parent organization(s) (as applicable) to ensure corporate leadership, the parent's systems, processes and independent assessments are used to assess the Contractor's performance. The purpose of NNSA oversight is for assessing the Contractor's performance in meeting its obligations under this Contract, in addition to measuring progress toward NNSA missions. The Contractor's accountability described in this clause is not reduced by the fact that NNSA conducts oversight activities.

(End of clause)

H-78 INSTRUCTIONS FOR UPDATING FOREIGN OWNERSHIP, CONTROL OR INFLUENCE (FOCI) INFORMATION (JUN 2011)

(a) In order to submit periodic updates or to report changes to Foreign Ownership, Control or Influence information as required by DEAR 952.204-2, Security, the Contractor shall use the DOE FOCI electronic submission system located at https://foci.anl.gov.

(b) New users, when registering to update information under this Contract, should select "NNSA Albuquerque Complex - Office of Partnership and Acquisition Services (NA-PAS)" as the FOCI Office that will review the FOCI Submission.

(c) All FOCI documentation/forms shall be completed within the eFOCI system. NOTE: A completed SF 328, Certificate Pertaining to Foreign Interests, executed in accordance with the instructions on the certification section of the SF328, shall be printed, signed and uploaded into the eFOCI system. The SF 328 is required for first time submissions, any time there are changes to the SF 328, and at the request of the Cognizant Security Authority (CSA). Specific problems maneuvering through the fields within the eFOCI system can be clarified by contacting the eFOCI help desk at (630) 252-6566 or fociserver@anl.gov.

(End of clause)

H-79 - LABORATORY, PLANT, AND SITE STRATEGIC PLANNING GUIDANCE

The Contractor shall submit to NNSA a laboratory, plant, or site strategic plan annually in accordance with the annual strategic planning guidance and the terms and conditions of the contract, or as directed by the Contracting Officer. The laboratory, plant, or site M&O leadership team shall present the site's plan and engage in discussions with senior NNSA and other M&O leadership as well as with key stakeholders (e.g., DOE and interagency partners) annually, if required in the annual strategic planning guidance, and as directed by the Contracting Officer.

(End of clause)

H-80 – CONTRACTOR PERFORMANCE EVALUATIONS

In accordance with Federal Acquisition Regulation (FAR) Subpart 42.15 Contractor Performance Information, the NNSA will prepare and submit past performance evaluations to the Past Performance Information Retrieval System (PPIRS). Evaluation reports will be documented not later than 120 days after the end of an evaluation period by using the Contractor Performance Assessment Reporting System (CPARS) which has connectivity with PPIRS. Contractor must register in CPARS in order to view/comment on their performance reports.

(End of clause)

H-81 –MITIGATING SUPPLY CHAIN RISK (OCT 2022)

DOE/NNSA utilizes a Supply Chain Risk Management (SCRM) Program to identify, assess, and monitor supply chain risks of critical vendors. The Government may use any information, public and non-public, including all-source intelligence for its analysis. The Contractor agrees that the Government may, at its own discretion, perform audits of supply chain risk processes or events consistent with other terms in the contract regarding access to records and audits. An onsite assessment may be required. Through the information obtained from a SCRM program, DOE may assess vendors and products through multiple risk lenses such as national security, cybersecurity, compliance, and finance. If supply chain risks are identified and corrective action becomes necessary, mutually agreeable corrective actions will be sought based upon specific

identified risks. Failure to resolve any identified risk may result in Contract termination.

(End of clause)

H-82 – MITIGATING SUPPLY CHAIN RISK USING ENHANCED PROCUREMENT AUTHORITY FOR INFORMATION AND COMMUNICATION TECHNOLOGY (OCT 2022)

(a) Definitions. As used in this clause–

Covered article - The term "covered article" includes-

(1) “Information technology” which means –

(i) any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency, if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency that requires the use-

(A) of that equipment, or

(B) of that equipment to a significant extent in the performance of a service or the furnishing of a product;

(ii) computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources; however,

(iii) does not include any equipment acquired by a federal contractor incidental to a federal contract.

(2) “Telecommunications Equipment”, which means equipment, other than customer premises equipment, used by a carrier to provide telecommunications services, and includes software integral to such equipment (including upgrades).

(3) “Telecommunications Service”, which means the offering of telecommunications for a fee directly to the public, or to such classes of users as to be effectively available directly to the public, regardless of the facilities used.

(4) the processing of information on a Federal or non-Federal information system, subject to the requirements of the Controlled Unclassified Information program; or

(5) hardware, systems, devices, software, or services that include embedded or incidental information technology.

Supply Chain Risk- The term "Supply Chain Risk" means the risk that a person may sabotage, maliciously introduce unwanted function, extract data, or otherwise manipulate the design, integrity, manufacturing, production, distribution, installation, operation, maintenance, disposition, or retirement of covered articles so as to surveil, deny, disrupt, or otherwise manipulate the function, use, or operation of the covered articles or information stored or transmitted on the covered articles.

(b) The Contractor shall take all prudent actions, and comply with all Government directions (as identified in (c)), to mitigate supply chain risk when providing covered articles or services affecting covered articles to the Government.

(c) In order to manage supply chain risk, the Government may use the authority provided by 41 U.S.C. 4713 to, among other things, withhold consent for the Contractor to subcontract with a particular source or direct the Contractor to exclude a particular source from consideration for a subcontract under the contract.

(d) Subcontracts. The Contractor shall insert the substance of this clause, including this paragraph (d), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items.

(End of clause)

H-83 – MITIGATING SUPPLY CHAIN RISK USING ENHANCED PROCUREMENT AUTHORITY FOR NATIONAL SECURITY SYSTEMS, NUCLEAR WEAPONS COMPONENTS AND ASSOCIATED ITEM (OCT 2022)

(a) Definitions. As used in this clause–

(1) "Covered system" means-

(A) National security systems (as defined at 44 U.S. Code § 3552) and components of such systems;

(B) Nuclear weapons and components of nuclear weapons;

(C) Items associated with the design, development, production, and maintenance of nuclear weapons or components of nuclear weapons;

(D) Items associated with the surveillance of the nuclear weapon stockpile; or

(E) Items associated with the design and development of nonproliferation and counterproliferation programs and systems.

(2) “Covered item of supply” means an item—

(A) that is purchased for inclusion in a covered system; and

(B) the loss of integrity of which could result in a supply chain risk for a covered system.

(3) “Supply Chain Risk” means the risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a covered system or covered item of supply so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of the system or item of supply.

(b) The Contractor shall take all prudent actions, and comply with all Government directions (as identified in (c)), to mitigate supply chain risk when providing covered systems or covered items of supply to the Government, and services affecting covered systems or covered items of supply.

(c) In order to manage supply chain risk, the Government may use the authority provided by 50 U.S.C. 2786, to, among other things, withhold of consent for the Contractor to subcontract with a particular source or direct the Contractor to exclude a particular source from consideration for a subcontract under the contract When the Government exercises this authority, it will only provide the Contractor with information pertaining to the basis of the action to the extent necessary to carry out the action. No action taken by the Government pursuant to 50 U.S.C. § 2786 shall be subject to review in any Federal court.

(d) Subcontracts. The Contractor shall insert the substance of this clause, including this paragraph (d), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items.

(End of clause)

H-84 SAFEGUARDING COVERED NNSA INFORMATION, CLOUD COMPUTING SERVICES, AND CYBERSECURITY INCIDENT REPORTING

(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/cloudservice-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 nondisclosure 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.

(End of clause)

C. Part II – Contract Clauses, Section I, I.40, DEAR 970.5215-1 Total Available Fee: Base Fee Amount and Performance Fee Amount (DEC 2000) ALTERNATE II (DEC 2000) ALTERNATE IV (DEC 2000) is deleted in its entirety and replaced as follows:

DEAR 970.5215-1 TOTAL AVAILABLE FEE: BASE FEE AMOUNT AND PERFORMANCE FEE AMOUNT (DEC 2024)

(a) Total available fee. Total available fee, consisting of a base fee amount (which may be zero) and a performance fee amount (consisting of an incentive fee component for objective performance requirements, an award fee component for subjective performance requirements, or both) determined in accordance with the provisions of this clause, is available for payment in accordance with the clause of this contract entitled, "Payments and advances."

(b) Fee negotiations. For any fee negotiations under this contract, at any time prior to the beginning of the evaluation period the negotiations cover, the Contracting Officer and Contractor shall attempt to reach agreement on: the requirements for the evaluation period including, if appropriate, the evaluation areas and individual requirements subject to incentives; the total available fee amount of the evaluation period; and the allocation of the total available fee amount. If agreement is reached prior to the beginning of the evaluation period, the Contracting Officer shall modify the contract to reflect the agreement. If agreement is not reached prior to the beginning of the evaluation period, the Contracting Officer will, prior to the beginning of the evaluation period, unilaterally determine: the requirements of the evaluation period including, if appropriate, the evaluation areas and individual requirements subject to incentives, the total available fee amount, and the allocation of the total available fee amount. The Contracting Officer shall modify the contract to reflect the determination.

(c) Determination of total available fee amount earned.

(1) The Department of Energy (DOE) shall, at the conclusion of each specified evaluation period, evaluate the Contractor's performance of all requirements, and determine the total available fee amount earned. At DOE's discretion, if the contact established specific incentivized requirements and a schedule for their completion and the Contractor completes them during the evaluation period, DOE may evaluate the Contractor's performance upon the requirements' completion. The Contractor agrees the determination of the total available fee amount earned is a unilateral determination made by the Fee Determining Official (FDO). DOE will identify the FDO. The FDO will be the DOE Operations/Field Office Manager, or another DOE official designated by the Assistant Secretary or equivalent (not delegable).

(2) If the award fee cycle consists of one evaluation period, award fee not earned during the evaluation period shall not be allocated to future evaluation periods. At the sole discretion of DOE, if the award fee cycle consists of more than one evaluation period, award fee not earned during the evaluation period may be allocated to future evaluation periods within the same award fee cycle.

(3) Following each evaluation period, the Contractor shall submit a self-assessment within seven calendar days after the end of the period. This self-assessment shall address both the strengths and weaknesses of the Contractor's performance during the evaluation period. Where deficiencies in performance are noted, the Contractor shall describe the actions planned or taken to correct them and avoid their recurrence. The FDO will review the Contractor's self-assessment as part of the evaluation of the Contractor's performance during the period.

(4) The FDO will evaluate the Contractor's performance in accordance with the Performance Evaluation and Measurement Plan (PEMP) described in paragraph (d) of this clause unless otherwise set forth in the contract. The Contractor shall be promptly advised in writing of the total available fee amount earned determination and the basis of the determination.

(d) PEMP. To the extent not set forth elsewhere in the contract:

(1) DOE shall establish a PEMP upon which the determination of the total available fee amount earned shall be based. The PEMP will address all of the requirements of contract performance specified in the contract directly or by reference. The Contracting Officer shall provide the Contractor with a copy of the PEMP before the start of an evaluation period.

(2) The PEMP will set forth the criteria upon which the Contractor will be evaluated relating to any technical, schedule, management, and/or cost objectives selected for evaluation. The PEMP will include, per 48 CFR 16.402-1, a cost incentive (or constraint). The criteria in the PEMP should be objective but may also include subjective criteria. The PEMP will set forth the method by which the total available fee amount will be allocated, and the total available fee amount earned will be determined.

(3) The PEMP may be revised, either unilaterally (by DOE) or bilaterally, during the evaluation period. If it is revised, the Contracting Officer shall notify the contractor—

(i) Of unilateral revisions (unless they are urgent and high priority) at least ninety calendar days prior to the end of the evaluation period and at least thirty calendar days prior to the effective date of the revision;

(ii) Of bilateral revisions (unless they are urgent and high priority) at least sixty calendar days prior to the end of the evaluation period;

(iii) Of urgent and high priority revisions, whether made unilaterally or bilaterally, at least thirty calendar days prior to the end of the evaluation period.

(e) Schedule for total available fee amount earned determinations. The FDO shall issue the final total available fee amount earned determination in accordance with the schedule set forth in the PEMP or as otherwise set forth in this contract.

(1) The determination for the evaluation period must be made within the later of: sixty calendar days after the receipt by the Contracting Officer of the Contractor's self-assessment, if one is required or permitted; seventy calendar days after the end of the evaluation period; or a longer period if the Contractor and Contracting Officer agree.

(2) If the FDO elects to evaluate the Contractor's performance of any specific requirements upon their completion, the determination of any fee amount earned must be made: within seventy calendar days of the requirements' completion; or a longer period if the Contractor and Contracting Officer agree.

(3) If the determination is not made within the periods stated above, the Contractor shall be entitled to interest on the total available fee amount earned at the rate established by the Secretary of the Treasury under section 12 of the Contract Disputes Act of 1978 (41 U.S.C. 7109) that is in effect on the payment date. This rate is referred to as the “Renegotiation Board Interest Rate,” and is published in the Federal Register semiannually on or about January 1 and July 1. The interest on any late total available fee amount earned determination will accrue daily and be compounded in 30-day increments inclusive from the first day after the schedule determination date through the actual date the determination is made. That is, interest accrued at the end of any 30-day period will be added to the total available fee amount earned and be subject to interest if not paid in the succeeding 30-day period.

(End of clause)

D. All other terms and conditions remain unchanged.

End of Modification 1117