



DEPARTMENT OF THE ARMY
U.S. ARMY CORPS OF ENGINEERS, LOUISVILLE DISTRICT
220 WEST MAIN STREET
LOUISVILLE, KY 40202

CELRL-CT

22 September 2026

Dear MATOC Contractors:

Reference is made to your Indefinite Delivery Indefinite Quantity (IDIQ) Multiple Award Task Order Contracts (MATOC), Numbers W912P523D0001 through W912P523D0007 to provide Design/Build Construction Services within the Great Lakes and Ohio River Division Mission Boundaries.

This letter serves as Amendment 0004 to Solicitation Number W912QR-62373550 for the Soo Lock Fire Alarm Modernization in Sault Sainte Marie, MI.

•See the attached Summary of Changes for Amendment 0004.

The basis for award of this task order is still lowest evaluated price. Please complete the price breakout schedule, to include the labor category table demonstrating the use of the binding rates included in your MATOC contract. The submitted price breakdown should include sufficient detail to allow the Government to verify that your proposed price incorporates the binding rates from your base contract. Any level of effort shown in the submitted information will not be used for evaluation purposes and will be used only to ensure that the proposal is in compliance with the binding rates from the base contract.

Offers providing less than 90 calendar days for Government acceptance after the due date of offers may not be considered and may be rejected.

The proposal due date remains 11:00 AM ET on 30 October 2026. Submit your proposal electronically through the Procurement Integrated Enterprise Environment (PIEE) solicitation module. Proposals not received by the stated date/time will not be considered. Please acknowledge receipt of this Amendment by signing below in the space provided and returning to Megan Murphy via email.

Payment and Performance Bonds will still be required for this project. The Notice to Proceed will be issued after receipt and approval of the bonds.

All questions regarding this Amendment as well as the entire solicitation must be submitted via ProjNet. The website to access this system is www.projnet.org and the bidder inquiry key for this specific project is: **CYF3NK-7ZP2UW.**

System for Award Management (SAM): Your SAM registration is required to be active at the time of proposal submission.

If you have contractual questions, please contact Megan Murphy via email at Megan.R.Murphy@usace.army.mil. If an Offeror believes that the requirements in the RFP contain an error, omission, or are otherwise unsound; the offeror shall immediately notify the Contract Specialist in writing with supporting rationale. The Offeror is reminded that the Government reserves the right to award this RFP based on the initial proposals, as received, without discussion.



Digitally signed by
DUGGINS.PATRICK.J.1230307578
Date: 2026.09.22 14:18:50 -04'00'

Patrick J. Duggins
Contracting Officer

W912QR-62373550 AMENDMENT 0004 ACKNOWLEDGEMENT:

(Signature)

(Date)

(Printed Name)

(Firm Name)

SUMMARY OF CHANGES

- A. The site visit information has been revised in Section 00 70 00.
- B. Offerors must acknowledge all amendments. All other terms and conditions remain unchanged.

End of Summary of Changes

Section 00 70 00

Prohibition on a ByteDance Covered Application.

As prescribed in 4.2203(c), insert the following clause:

Prohibition on a ByteDance *Covered Application* (Jun 2023)

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

Covered application means the social networking service TikTok or any successor application or service developed or provided by ByteDance Limited or an entity owned by ByteDance Limited.

Information technology, as defined in 40 U.S.C. 11101(6)-

(1) Means 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-

(i) Of that equipment; or

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

(2) Includes 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; but

(3) Does not include any equipment acquired by a Federal contractor incidental to a Federal contract.

(b) *Prohibition*. Section 102 of Division R of the Consolidated Appropriations Act, 2023 (Pub. L. 117-328), the No TikTok on Government Devices Act, and its implementing guidance under Office of Management and Budget (OMB) Memorandum M-23-13, dated February 27, 2023, "No TikTok on Government Devices" Implementation Guidance, collectively prohibit the presence or use of a *covered application* on *executive agency information technology*, including certain equipment used by Federal contractors. The Contractor is prohibited from having or using a *covered application* on any *information technology* owned or managed by the

Government, or on any *information technology* used or provided by the Contractor under this contract, including equipment provided by the Contractor's employees; however, this prohibition does not apply if the *Contracting Officer* provides written notification to the Contractor that an exception has been granted in accordance with OMB Memorandum M-23-13.

(c) *Subcontracts*. The Contractor *shall* insert the substance of this clause, including this paragraph (c), in all subcontracts, including subcontracts for the *acquisition of commercial products or commercial services*.

(End of clause)

Commencement, Prosecution, and Completion of Work (Apr 1984)

The Contractor shall be required to

(a) commence work under this contract within 10 calendar days after the date the Contractor receives the notice to proceed,

(b) prosecute the work diligently, and

(c) complete the entire work ready for use not later than 365 calendar days from Notice to Proceed. The time stated for completion shall include final cleanup of the premises.

(End of Clause)

52.211-12 Liquidated Damages -- Construction (Sept 2000)

(a) If the Contractor fails to complete the work within the time specified in the contract, the Contractor shall pay liquidated damages to the Government in the amount of \$5,175.00 for each calendar day of delay until the work is completed or accepted.

(b) If the Government terminates the Contractor's right to proceed, liquidated damages will continue to accrue until the work is completed. These liquidated damages are in addition to excess costs of repurchase under the Termination clause.

(End of Clause)

52.211-13 TIME EXTENSIONS (SEPT 2000)

Time extensions for contract changes will depend upon the extent, if any, by which the changes cause delay in the completion of the various elements of construction. The change order granting the time extension may provide that the contract completion date will be extended only for those specific elements related to the changed work and that the remaining contract completion dates

for all other portions of the work will not be altered. The change order also may provide an equitable readjustment of liquidated damages under the new completion schedule.

(End of clause)

PERFORMANCE OF WORK BY THE CONTRACTOR (APR 1984)

The Contractor shall perform on the site, and with its own organization, work equivalent to at least twenty (20) percent of the total amount of work to be performed under the contract. This percentage may be reduced by a supplemental agreement to this contract if, during performing the work, the Contractor requests a reduction and the Contracting Officer determines that the reduction would be to the advantage of the Government.

(End of clause)

Physical Data (Apr 1984)

Data and information furnished or referred to below is for the Contractor's information. The Government shall not be responsible for any interpretation of or conclusion drawn from the data or information by the Contractor.

(a) The indications of physical conditions on the drawings and in the specifications are the result of site investigations.

(b) Weather conditions: The Contractor shall make his own investigations as to weather conditions at the site. Data may be obtained from various National Weather Service offices located generally at airports of principal cities, the nearest to this project being Sault St Marie, MI.

(c) Transportation facilities: Roads and railroads in the general area are not shown on the drawings. Access ways shall be investigated by the Contractor to satisfy himself as to their existence and allowable use.

(d) Historical data for all areas may be obtained from:

U. S. Department of Commerce
National Climatic Center
Federal Building
Asheville, N. C. 28801

(End of Clause)

*****AMENDMENT 0004*****

Site Visit (Construction) (Feb 1995) Alternate I

(a) The clauses at [52.236-2](#), Differing Site Conditions, and [52.236-3](#), Site Investigations and Conditions Affecting the Work, will be included in any contract awarded as a result of this

solicitation. Accordingly, offerors or quoters are urged and expected to inspect the site where the work will be performed.

Coordinate with on-site PM, Marcy Werth via email (Marcy.J.Werth2@usace.army.mil) or by phone: (716) 359-1035 on the following:

Site Visit Information:

DATE: Tuesday, 06 OCT 2026

TIME: 9:00 AM Local Time

LOCATION: Meet at Soo Locks Main Guard Gate on W. Portage Avenue, Sault Sainte Marie, Michigan.

POC: Eric Galer or Andrew Nelson

At least 2 working days prior to the site visit (02 OCT), the following information must be submitted via email to Marcy.J.Werth2@usace.army.mil to facilitate entry access. If your information is received after the deadline, we will not be able to guarantee you site access. Anyone planning to attend the site visit must submit the following:

- For US citizens: Full name, date of birth, social security number, and their company name
- For Non-US Citizens: Full name, date of birth, passport number, and their company name

Due to ongoing active construction at the Soo Locks, PPE will be required by all attendees. Required PPE includes, at a minimum, hard hat, safety glasses, high visibility vest (Class II minimum), and hard toe boots/shoes. Some loaner PPE may be available, but attendees should plan to bring their own. NOTE: If any site visit attendee(s) would like to view the deep service tunnel, prior to being allowed access, they will need to show proof of fall protection training and confined space training.

(End of provision)

*****AMENDMENT 0004*****

52.246-21 WARRANTY OF CONSTRUCTION (MAR 1994)

(a) In addition to any other warranties in this contract, the Contractor warrants, except as provided in paragraph (i) of this clause, that work performed under this contract conforms to the contract requirements and is free of any defect in equipment, material, or design furnished, or workmanship performed by the Contractor or any subcontractor or supplier at any tier.

(b) This warranty shall continue for a period of 1 year from the date of final acceptance of the work. If the Government takes possession of any part of the work before final acceptance, this warranty shall continue for a period of 1 year from the date the Government takes possession.

(c)The Contractor shall remedy at the Contractor's expense any failure to conform, or any defect. In addition, the Contractor shall remedy at the Contractor's expense any damage to Government-owned or controlled real or personal property, when that damage is the result of-

(1)The Contractor's failure to conform to contract requirements; or

(2)Any defect of equipment, material, workmanship, or design furnished.

(d)The Contractor shall restore any work damaged in fulfilling the terms and conditions of this clause. The Contractor's warranty with respect to work repaired or replaced will run for 1 year from the date of repair or replacement.

(e)The Contracting Officer shall notify the Contractor, in writing, within a reasonable time after the discovery of any failure, defect, or damage.

(f)If the Contractor fails to remedy any failure, defect, or damage within a reasonable time after receipt of notice, the Government shall have the right to replace, repair, or otherwise remedy the failure, defect, or damage at the Contractor's expense.

(g)With respect to all warranties, express or implied, from subcontractors, manufacturers, or suppliers for work performed and materials furnished under this contract, the Contractor shall-

(1)Obtain all warranties that would be given in normal commercial practice;

(2)Require all warranties to be executed, in writing, for the benefit of the Government, if directed by the Contracting Officer; and

(3)Enforce all warranties for the benefit of the Government, if directed by the Contracting Officer.

(h)In the event the Contractor's warranty under paragraph (b) of this clause has expired, the Government may bring suit at its expense to enforce a subcontractor's, manufacturer's, or supplier's warranty.

(i)Unless a defect is caused by the negligence of the Contractor or subcontractor or supplier at any tier, the Contractor shall not be liable for the repair of any defects of material or design furnished by the Government nor for the repair of any damage that results from any defect in Government-furnished material or design.

(j)This warranty shall not limit the Government's rights under the Inspection and Acceptance clause of this contract with respect to latent defects, gross mistakes, or fraud.

(End of clause)

252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting

**SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT
REPORTING (MAY 2024)**

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

“Adequate security” means protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information.

“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 attributional/proprietary information” means information that identifies the contractor(s), whether directly or indirectly, by the grouping of information that can be traced back to the contractor(s) (e.g., program description, facility locations), personally identifiable information, as well as trade secrets, commercial or financial information, or other commercially sensitive information that is not customarily shared outside of the company.

“Controlled technical information” means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information would meet the criteria, if disseminated, for distribution statements B through F using the criteria set forth in DoD Instruction 5230.24, Distribution Statements on Technical Documents. The term does not include information that is lawfully publicly available without restrictions.

“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 defense information.

“Covered defense information” means unclassified controlled technical information or other information, as described in the Controlled Unclassified Information (CUI) Registry at <http://www.archives.gov/cui/registry/category-list.html>, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, 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 DoD 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.

“Cyber 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.

“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 defense information is recorded, stored, or printed within a covered contractor information system.

“Operationally critical support” means supplies or services designated by the Government as critical for airlift, sealift, intermodal transportation services, or logistical support that is essential to the mobilization, deployment, or sustainment of the Armed Forces in a contingency operation.

“Rapidly report” means within 72 hours of discovery of any cyber incident.

“Technical information” means technical data or computer software, as those terms are defined in the clause at DFARS [252.227-7013](#), Rights in Technical Data—Other Than Commercial Products and Commercial Services, regardless of whether or not the clause is incorporated in this solicitation or contract. Examples of technical information include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.

(b) *Adequate security*. The Contractor shall provide adequate security on all covered contractor information systems. To provide adequate 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 specified in the clause [252.239-7010](#), Cloud Computing Services, of this contract.

(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 covered contractor information system shall be subject to the security requirements 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/sp800>) in effect at the time the solicitation is issued or as authorized by the Contracting Officer.

(ii)(A) The Contractor shall implement NIST SP 800-171, as soon as practical, but not later than December 31, 2017. For all contracts awarded prior to October 1, 2017, the Contractor shall notify the DoD Chief Information Officer (CIO), via email at osd.dibcsia@mail.mil, within 30 days of contract award, of any security requirements specified by NIST SP 800-171 not implemented at the time of contract award.

(B) The Contractor shall submit requests to vary from NIST SP 800-171 in writing to the Contracting Officer, for consideration by the DoD CIO. The Contractor need not implement any security requirement adjudicated by an authorized representative of the DoD CIO to be nonapplicable or to have an alternative, but equally effective, security measure that may be implemented in its place.

(C) If the DoD CIO has previously adjudicated the contractor's requests indicating that a requirement is not applicable or that an alternative security measure is equally effective, a copy of that approval shall be provided to the Contracting Officer when requesting its recognition under this contract.

(D) If the Contractor intends to use an external cloud service provider to store, process, or transmit any covered defense 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) Moderate baseline (<https://www.fedramp.gov/documents-templates/>) and that the cloud service provider complies with requirements in paragraphs (c) through (g) of this clause for cyber incident reporting, malicious software, media preservation and protection, access to additional information and equipment necessary for forensic analysis, and cyber incident damage assessment.

(3) Apply other information systems security measures when the Contractor reasonably determines that information systems security measures, in addition to those identified in paragraphs (b)(1) and (2) of this clause, may be required to provide adequate 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 may be addressed in a system security plan.

(c) Cyber incident reporting requirement.

(1) When the Contractor discovers a cyber incident that affects a covered contractor information system or the covered defense information residing therein, or that 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 defense 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 cyber 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 defense information, or that affect the Contractor's ability to provide operationally critical support; and

(ii) Rapidly report cyber incidents to DoD at <https://dibnet.dod.mil>.

(2) *Cyber incident report.* The cyber incident report shall be treated as information created by or for DoD and shall include, at a minimum, the required elements at <https://dibnet.dod.mil>.

(3) *Medium assurance certificate requirement.* In order to report cyber incidents in accordance with this clause, the Contractor or subcontractor shall have or acquire a DoD-approved medium assurance certificate to report cyber incidents. For information on obtaining a DoD-approved medium assurance certificate, see <https://public.cyber.mil/eca/>.

(d) *Malicious software.* When the Contractor or subcontractors discover and isolate malicious software in connection with a reported cyber incident, submit the malicious software to DoD Cyber Crime Center (DC3) in accordance with instructions provided by DC3 or the Contracting Officer. Do not send the malicious software to the Contracting Officer.

(e) *Media preservation and protection.* When a Contractor discovers a cyber 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 90 days from the submission of the cyber incident report to allow DoD to request the media or decline interest.

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

(g) *Cyber incident damage assessment activities.* If DoD 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) *DoD safeguarding and use of contractor attributional/proprietary information.* 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 attributional/proprietary information, including such information submitted in accordance with paragraph (c). To the maximum extent practicable, the Contractor shall identify and mark attributional/proprietary information. In making an authorized release of such information, the Government will implement appropriate procedures to minimize the contractor attributional/proprietary information that is included in such authorized release, seeking to include only that information that is necessary for the authorized purpose(s) for which the information is being released.

(i) *Use and release of contractor attributional/proprietary information not created by or for DoD.* 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 DoD is authorized to be released outside of DoD—

(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 cyber incidents;

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

(4) For national security purposes, including cyber situational awareness and defense purposes (including with Defense Industrial Base (DIB) participants in the program at 32 CFR part 236); or

(5) To a support services contractor (“recipient”) that is directly supporting Government activities under a contract that includes the clause at [252.204-7009](#), Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information.

(j) *Use and release of contractor attributional/proprietary information created by or for DoD.* Information that is obtained from the contractor (or derived from information obtained from the contractor) under this clause that is created by or for DoD (including the information submitted pursuant to paragraph (c) of this clause) is authorized to be used and released outside of DoD 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 cyber incident reporting required by this clause in no way abrogates the Contractor’s responsibility for other safeguarding or cyber 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) *Subcontracts.* The Contractor shall—

(1) Include this clause, including this paragraph (m), in subcontracts, or similar contractual instruments, for operationally critical support, or for which subcontract performance will involve covered defense information, 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 defense information and will require protection under this clause, and, if necessary, consult with the Contracting Officer; and

(2) Require subcontractors to—

(i) Notify the prime Contractor (or next higher-tier subcontractor) when submitting a request to vary from a NIST SP 800-171 security requirement to the Contracting Officer, in accordance with paragraph (b)(2)(ii)(B) of this clause; and

(ii) Provide the incident report number, automatically assigned by DoD, to the prime Contractor (or next higher-tier subcontractor) as soon as practicable, when reporting a cyber incident to DoD as required in paragraph (c) of this clause.

(End of clause)

252.204-7021 Contractor Compliance With the Cybersecurity Maturity Model Certification Level Requirements

CONTRACTOR COMPLIANCE WITH THE CYBERSECURITY MATURITY MODEL CERTIFICATION LEVEL REQUIREMENTS (NOV 2025)

(a) Definitions. As used in this clause—

“Controlled unclassified information” means information the Government creates or possesses, or information an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Governmentwide policy requires or permits an agency to handle using safeguarding or dissemination controls (32 CFR 2002.4(h)).

“Current” means—

(1) With regard to Conditional Cybersecurity Maturity Model Certification (CMMC) Status—

(i) Not older than 180 days for Conditional Level 2 (Self) assessments and Conditional Level 2 (certified third-party assessment organization (C3PAO)) assessments, with—

(A) No changes in compliance with the requirements at 32 CFR part 170 since the Conditional CMMC Status date (see 32 CFR 170.16 and 170.17); and

(B) A corresponding affirmation of continuous compliance by an affirming official (see 32 CFR 170.4); and

(ii) Not older than 180 days for Conditional Level 3 (Defense Industrial Base Cybersecurity Assessment Center (DIBCAC)) assessments, with—

(A) No changes in compliance with the requirements at 32 CFR part 170 since the Conditional CMMC Status date (see 32 CFR 170.18); and

(B) A corresponding affirmation of continuous compliance by an affirming official;

(2) With regard to Final CMMC Status—

(i) Not older than 1 year for Final Level 1 (Self), with—

(A) No changes in compliance with the requirements at 32 CFR part 170 since the Final CMMC Status date (see 32 CFR 170.15); and

(B) A corresponding affirmation of continuous compliance, not older than 1 year, by an affirming official;

(ii) Not older than 3 years for Final Level 2 (Self) assessments and Final Level 2 (C3PAO) assessments, with—

(A) No changes in compliance with the requirements at 32 CFR part 170 since the Final CMMC Status date (see 32 CFR 170.16 and 170.17); and

(B) A corresponding affirmation of continuous compliance, not older than 1 year, by an affirming official; and

(iii) Not older than 3 years for Final Level 3 (DIBCAC) assessments, with—

(A) No changes in compliance with the requirements at 32 CFR part 170 since the Final CMMC Status date (see 32 CFR 170.18); and

(B) A corresponding affirmation of continuous compliance, not older than 1 year, by an affirming official; and

(3) With regard to affirmation of continuous compliance (32 CFR 170.22), not older than 1 year with no changes in compliance with the requirements at 32 CFR part 170.

“Cybersecurity Maturity Model Certification (CMMC) status” means the result of meeting or exceeding the minimum required score for the corresponding assessment. The potential statuses are as follows:

(1) Final Level 1 (Self).

(2) Conditional Level 2 (Self).

(3) Final Level 2 (Self).

(4) Conditional Level 2 (C3PAO).

(5) Final Level 2 (C3PAO).

(6) Conditional Level 3 (DIBCAC).

(7) Final Level 3 (DIBCAC).

“Cybersecurity Maturity Model Certification unique identifier (CMMC UID)” means 10 alphanumeric characters assigned to each CMMC assessment and reflected in the Supplier Performance Risk System (SPRS) for each contractor information system.

“Federal contract information (FCI)” 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. It does not include information provided by the Government to the public, such as on public websites, or simple transactional information, such as information necessary to process payments.

“Plan of action and milestones” means a document that identifies tasks to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and

scheduled completion dates for the milestones, as defined in National Institute of Standards and Technology Special Publication 800-115 (32 CFR 170.21).

(b) Framework. The Cybersecurity Maturity Model Certification (CMMC) is a framework for assessing a contractor's compliance with applicable information security protections (see 32 CFR part 170).

(c) Duplication. The CMMC assessments will not duplicate efforts from any other comparable DoD assessment, except for rare circumstances when a reassessment may be necessary, for example, when there are indications of issues with cybersecurity and/or compliance with CMMC requirements.

(d) *Requirements.* The Contractor shall—

(1)(i) Have and maintain for the duration of the contract a current CMMC status at the following CMMC level, or higher: CMMC Level 2 (Self) for all information systems used in performance of the contract, task order, or delivery order that process, store, or transmit FCI or CUI; and

(ii) Consult 32 CFR 170.23 related to the flowdown of the CMMC requirements, and flow down the correct CMMC level to subcontracts and other contractual instruments;

(2) Only process, store, or transmit FCI or CUI on contractor information systems that have a CMMC status at the CMMC level required in paragraph (d)(1) of this clause, or higher;

(3) Complete on an annual basis, and maintain as current, an affirmation, by the affirming official (see 32 CFR 170.4), of continuous compliance with the requirements associated with the CMMC level required in paragraph (d)(1) of this clause in the Supplier Performance Risk System (SPRS) (<https://piee.eb.mil>) for each CMMC UID applicable to each of the contractor information systems that process, store, or transmit FCI or CUI and that are used in performance of the contract;

(4) Ensure all subcontractors and suppliers complete prior to subcontract award, and maintain on an annual basis, an affirmation, by the affirming official (see 32 CFR 170.4), of continuous compliance with the requirements associated with the CMMC level required for the subcontract or other contractual instrument for each of the subcontractor information systems that process, store, or transmit FCI or CUI and that are used in performance of the subcontract; and

(5) If the Contractor has a CMMC Status of Conditional, successfully close out a valid plan of action and milestones (32 CFR 170.21) to achieve a CMMC Status of Final.

(e) Reporting. The Contractor shall—

(1) Submit to the Contracting Officer—

(i) The CMMC UID(s) issued by SPRS for contractor information systems that will process, store, or transmit FCI or CUI during performance of the contract; and

(ii) Any changes in the CMMC UIDs generated in SPRS throughout the life of the contract, task order, or delivery order, if applicable;

(2) Enter into SPRS the results of a current self-assessment for each CMMC UID, not covered by a C3PAO assessment or DIBCAC assessment, applicable to each of the contractor information systems that process, store, or transmit FCI or CUI and that are used in performance of the contract; and

(3) Complete in SPRS on an annual basis and maintain as current an affirmation of continuous compliance by the affirming official (see 32 CFR 170.4) for each self-assessment, C3PAO assessment, or DIBCAC assessment required under the contract in SPRS.

(f) *Subcontracts*. The Contractor shall—

(1) Insert the substance of this clause, including this paragraph (f) and excluding paragraph (e)(1), in subcontracts and other contractual instruments, including those for the acquisition of commercial products and commercial services, excluding commercially available off-the-shelf items , if the subcontract or other contractual instrument will contain a requirement to process, store, or transmit FCI or CUI; and

(2) Prior to awarding a subcontract or other contractual instrument, ensure that the subcontractor has a current CMMC certificate or current CMMC status at the CMMC level that is appropriate for the information that is being flowed down to the subcontractor based on the requirements at 32 CFR 170.23.

(End of clause)

252.204-7024 Notice on the Use of the Supplier Performance Risk System

NOTICE ON THE USE OF THE SUPPLIER PERFORMANCE RISK SYSTEM (MAR 2023)

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

“Item risk” means the probability that a product, based on intended use, will introduce performance risk resulting in safety issues, mission degradation, or monetary loss.

“Price risk” means a measure of whether a proposed price for a product or service is consistent with historical prices paid for that item or service.

“Supplier risk” means the probability that an award may subject the procurement to the risk of unsuccessful performance or to supply chain risk (see Defense Federal Acquisition Regulation Supplement [239.7301](#)).

(b) The Supplier Performance Risk System (SPRS), available at <https://piee.eb.mil/>, will be used in the evaluation of the Quoter or Offeror’s performance. SPRS retrieves item, price, quality, delivery, and contractor information on contracts from Government reporting systems in order to develop risk assessments.

(c) The Contracting Officer will consider SPRS risk assessments during the evaluation of quotations or offers received in response to this solicitation as follows:

(1) Item risk will be considered to determine whether the procurement represents a high performance risk to the Government.

(2) Price risk will be considered in determining if a proposed price is consistent with historical prices paid for a product or a service or otherwise creates a risk to the Government.

(3) Supplier risk, including but not limited to quality and delivery, will be considered to assess the risk of unsuccessful performance and supply chain risk.

(d) SPRS risk assessments are generated daily. Quoters or Offerors are able to access their risk assessments by following the access instructions in the SPRS user's guide available at <https://www.sprs.csd.disa.mil/reference.htm>. Quoters and Offerors are granted access to SPRS for their own risk assessment classifications only. SPRS reporting procedures and risk assessment methodology are detailed in the SPRS user's guide. The method to challenge a rating generated by SPRS is also provided in the user's guide. SPRS evaluation criteria are available at https://www.sprs.csd.disa.mil/pdf/SPRS_DataEvaluationCriteria.pdf.

(e) The Contracting Officer may consider any other available and relevant information when evaluating a quotation or an offer.

(End of provision)

252.204-7025 Notice of Cybersecurity Maturity Model Certification Level Requirements 2025-11

NOTICE OF CYBERSECURITY MATURITY MODEL CERTIFICATION LEVEL REQUIREMENTS (NOV 2025)

(a) Definitions. As used in this provision, "controlled unclassified information (CUI)," "current," "Cybersecurity Maturity Model Certification (CMMC) status," "Cybersecurity Maturity Model Certification unique identifier (CMMC UID)," "Federal contract information (FCI)," and "plan of action and milestones" have the meaning given in the Defense Federal Acquisition Regulation Supplement 252.204-7021, Contractor Compliance With the Cybersecurity Maturity Model Certification Level Requirements, clause of this solicitation.

b)(1) Cybersecurity Maturity Model Certification (CMMC) level. The CMMC level required by this solicitation is: CMMC Level 2 (Self). This CMMC level, or higher (see 32 CFR part 170), is required prior to award for each contractor information system that will process, store, or transmit Federal contract information (FCI) or controlled unclassified information (CUI) during performance of the contract.

(2) The Offeror will not be eligible for award of a contract, task order, or delivery order resulting from this solicitation if the Offeror does not have, for each of the contractor information systems that will process, store, or transmit FCI or CUI and that will be used in performance of a contract resulting from this solicitation-

(i) The current CMMC status entered in the Supplier Performance Risk System (SPRS) (<https://piee.eb.mil>) at the CMMC level required by paragraph (b)(1) of this provision; and

(ii) A current affirmation of continuous compliance with the security requirements identified at 32 CFR part 170 in SPRS.

(c) Plan of action and milestones. If the Offeror has a CMMC Status of Conditional, the Offeror shall successfully close out a valid plan of action and milestones (32 CFR 170.21) to achieve a CMMC Status of Final.

(d) CMMC unique identifiers. The Offeror shall provide, in the proposal, the CMMC unique identifier(s) (CMMC UIDs) issued by SPRS for each contractor information system that will process, store, or transmit FCI or CUI during performance of a contract, task order, or delivery order resulting from this solicitation. The Offeror also shall update the list when new CMMC UIDs are generated in SPRS. The CMMC UIDs are provided in SPRS after the Offeror enters the results of self-assessment(s) for each such information system.

(End of provision)

252.236-7001 Contract Drawings and Specifications (AUG 2000)

(a) The Government will provide to the Contractor, without charge, one set of contract drawings and specifications, except publications incorporated into the technical provisions by reference, in electronic or paper media as chosen by the Contracting Officer.

(b) The Contractor shall—

- (1) Check all drawings furnished immediately upon receipt;
- (2) Compare all drawings and verify the figures before laying out the work;
- (3) Promptly notify the Contracting Officer of any discrepancies;
- (4) Be responsible for any errors that might have been avoided by complying with this paragraph (b); and
- (5) Reproduce and print contract drawings and specifications as needed.

(c) In general--

- (1) Large-scale drawings shall govern small-scale drawings; and
- (2) The Contractor shall follow figures marked on drawings in preference to scale measurements.

(d) Omissions from the drawings or specifications or the misdescription of details of work that are manifestly necessary to carry out the intent of the drawings and specifications, or that are customarily performed, shall not relieve the Contractor from performing such omitted or misdescribed details of the work. The Contractor shall perform such details as if fully and correctly set forth and described in the drawings and specifications.

(e) The work shall conform to the specifications and the contract drawings identified on the following index of drawings:

Attachment A, Sheet G-001

(End of clause)

UAI 5152.236-9011 DESIGN-BUILD CONSTRUCTION CONTRACTS (MAR 2019)

(a) Design-Build Contract Order of Precedence. The contract includes the standard contract clauses and schedules current at the time of contract award. It entails (1) the Solicitation in its entirety, including all drawings, cuts, and illustrations, and any amendments, and (2) the successful offeror's accepted proposal. The contract constitutes and defines the entire agreement between the Contractor and the Government. No documentation shall be omitted which in any way bears upon the terms of that agreement.

(1) In the event of conflict or inconsistency between any portion of this contract, precedence shall be given in the following order:

i. Betterments: Any portions of the accepted proposal which both conform to and exceed the requirements of the Solicitation.

ii. The requirements of the Solicitation. (See also FAR 52.236-21, Specifications and Drawings for Construction)

iii. All other elements of the accepted proposal.

iv. Any design products including, but not limited to, plans, specifications, engineering studies and analyses, shop drawings, equipment installation drawings, etc. These are "deliverables" under the contract and are not part of the contract itself. Design products must conform to all provisions of the contract, in the order of precedence herein.

(b) Personnel, subcontractors, and outside associates or consultants. In connection with this contract, any in-house personnel, subcontractors, and outside associates or consultants will be limited to individuals or firms that were specifically identified in the Contractor's accepted proposal. The Contractor shall obtain the Contracting Officer's written consent before making any substitution for these designated in-house personnel, subcontractors, associates, or consultants. If the Contractor proposes a substitution, it shall submit the same type of information that was submitted in the accepted proposal to the Contracting Officer for evaluation and approval. The level of qualifications and experience submitted in the accepted proposal or that required by the Solicitation, whichever is greater, is the minimum standard for any substitution.

(c) Responsibility of the Contractor for Design. The Contractor shall be responsible for the professional quality, technical accuracy, and the coordination of all designs, drawings, specifications, and other non-construction services furnished by the Contractor under this contract. The Contractor shall, without additional compensation, correct or revise any errors or deficiency in its designs, drawings, specifications, and other non-construction services and perform any necessary rework or modifications, including any damage to real or personal property, resulting from the design error or omission.

(1) The standard of care for all design services performed under this agreement shall be the care and skill ordinarily used by members of the architectural or engineering professions practicing under similar conditions at the same time and locality. Notwithstanding the above, in the event that the contract specifies that portions of the Work be performed in accordance with a performance standard, the design services shall be performed so as to achieve such standards.

(2) Neither the Government's review, approval or acceptance of, nor payment for, the services required under this contract, shall be construed to operate as a waiver of any rights under this contract or of any cause of action arising out of the performance of this contract. The Contractor shall be and remain liable to the Government in accordance with applicable law for all damages to the Government caused by the Contractor's negligent performance of any of these services furnished under this contract.

(3) The rights and remedies of the Government provided for under this contract are in addition to any other rights and remedies provided by law.

(4) If the Contractor is comprised of more than one legal entity, each entity shall be jointly and severally liable hereunder.

(d) Contractor's Role during the Design Process. The Contractor's construction management key personnel shall be actively involved during the design process to effectively integrate the design and construction requirements of this contract. In addition to the typical required construction activities, the Contractor's involvement includes, but is not limited to actions such as: integrating the design schedule into the Master Schedule to maximize the effectiveness of fast-tracking design and construction (within the limits allowed in the contract), ensuring constructability and economy of the design, integrating the shop drawing and installation drawing process into the design, executing the material and equipment acquisition programs to meet critical schedules, effectively interfacing the design and construction quality control (QC) management programs with the design QC program, and maintaining and providing the design team with accurate, up-to-date redline and as-built documentation for eventual submission as Record Drawings.. The Contractor shall require and manage the active involvement of key trade subcontractors in the above activities.

(e) Deviating from the Accepted Design. The Contractor must obtain the approval of the Designer of Record and the Government's concurrence, in the form of supplemental agreement to the contract, for any Contractor-proposed revision to the professionally stamped-and-sealed and Government-reviewed final design that has been released for Construction before proceeding with the revision. The Government reserves the right to disapprove such a revision.

(1) The Government reserves the right to non-concur with any revision to the final design that has been released for construction, including those which may impact furniture, furnishings, equipment selections or operations decisions that were made, based on the reviewed design.

(2) Any Contractor-proposed revision to the design which deviates from the contract requirements (i.e., the Request for Proposal (RFP) and the accepted proposal), will require a bilateral modification (e.g. supplemental agreement) to the contract before any work commences.

(3) Unless the Government initiates a change to the contract requirements, or the Government determines that the Government furnished design criteria are incorrect and must be revised, any Contractor initiated proposed change to the contract requirements, which results in additional cost, shall strictly be at the Contractor's expense.

(4) The Contractor shall track all approved revisions to the reviewed and accepted design and shall incorporate them into the as-built design documentation, in accordance with agreed procedures. The Designer of Record shall document its professional concurrence on the as-builts for any revisions in the stamped and sealed drawings and specifications.

(f) Value Engineering after Award. In reference to Federal Acquisition Regulation (FAR) 52.248-3, Value Engineering - Construction, the Government may refuse to entertain a "Value Engineering Change Proposal" (VECP) for those "performance oriented" aspects of the Solicitation documents which were addressed in the Contractor's accepted contract proposal and which were evaluated in competition with other offerors for award of this contract.

(1) The Government may consider a VECP for those "prescriptive" aspects of the Solicitation documents, not addressed in the Contractor's accepted contract proposal or addressed but evaluated only for minimum conformance with the Solicitation requirements.

(2) For purposes of this clause, the term "performance oriented" refers to those aspects of the design criteria or other contract requirements, which allow the offeror or Contractor certain latitude, choice of and flexibility to propose in its accepted proposal a choice of design, technical approach, design solution, construction approach or other approach to fulfill the contract requirements. Such requirements generally tend to be expressed in terms of functions to be performed, performance required or essential physical characteristics, without dictating a specific process or specific design solution for achieving the desired result.

(3) In contrast, for purposes of this clause, the term "prescriptive" refers to those aspects of the design criteria or other Solicitation requirements wherein the Government expressed the design solution or other requirements in terms of specific material, approaches, systems, and/or processes to be used. Prescriptive aspects typically allow the offerors little or no freedom in the choice of design approach, materials, fabrication techniques, methods of installation, or any other approach to fulfill the contract requirements.

(g) Warranty of Design. The Contractor warrants that the design shall be performed in accordance with the contract requirements. Design and design related construction not conforming to the Contract requirements shall be corrected at no additional cost to the Government. The standard of care for design is defined in paragraph c of this clause, Responsibility of the Contractor for Design.

(1) The period of this warranty shall commence upon final completion and the Government's acceptance of the work, or in the case of the Government's beneficial occupancy of all or part of the work for its convenience, prior to final completion and acceptance, at the time of such occupancy.

(2) This design warranty shall be effective from the above event through the Statute of Limitations and Statute of Repose or host nation law, as applicable to the place of construction performance.

(3) The rights and remedies of the Government provided for under this clause are in addition to any other rights and remedies provided in this contract or by law.

(h) Government Re-Use of Design. In conjunction with the Defense Federal Acquisition Regulation Supplement (DFARS) 252.227-7022, Government Rights (Unlimited), the Government will not ask for additional originals or copies of the design works after the Contractor provides all required design documentation and record drawing documentation under the instant contract. Further, if the Government uses the design for other projects without additional compensation to the Contractor for re-use, the Government releases the Contractor from liability in the design on the other projects, due to defects in the design that are not the result of fraud, gross mistake as amounts to fraud, gross negligence or intentional misrepresentation.

(End of clause)