ARTICLE IV: SAFEGUARDING CONTROLLED UNCLASSIFIED INFORMATION AND CONTROLLED TECHNICAL INFORMATION AND CYBER INCIDENT REPORTING

A. Background

Protection of Controlled Unclassified Information (CUI) and Controlled Technical Information (CTI) is of paramount importance to SDA and can directly impact the ability of SDA to successfully conduct its mission. Therefore, this Article requires Seller to protect CUI and CTI that resides on Seller's information systems. This article also requires Seller to rapidly report any cyber incident involving CUI or CTI.

B. Safeguarding CUI and CTI

Seller shall implement the version of NIST Special Publication (SP) 800-171 in effect at the time the solicitation is issued or as authorized by the Agreements Officer for CUI and CTI that resides on Seller's information systems. Consistent with NIST SP 800-171, implementation may be tailored to facilitate equivalent safeguarding measures used in Seller systems and organization. Any suspected loss or compromise of CUI or CTI that resides on Seller's information systems shall be considered a cyber incident and require Seller to rapidly report the incident to SDA in accordance with paragraph C below. Seller shall implement and maintain administrative, technical, and physical safeguards and controls with the security level and services required in accordance with the Cloud Computing Security Requirements Guide (SRG) (version in effect at the time the solicitation is issued or as authorized by the Agreements Officer) found at https://public.cyber.mil/dccs/dccs-documents/, unless notified by the Agreements Officer that this requirement has been waived by the DoD Chief Information Officer.

C. Cyber Incident Reporting

Upon discovery of a cyber incident involving CUI or CTI, Seller shall take immediate steps to mitigate any further loss or compromise. Seller shall rapidly report the incident to SDA and provide sufficient details of the event—including identification of detected and isolated malicious software—to enable SDA to assess the situation and provide feedback to Seller regarding further reporting and potential mitigation actions. Seller shall preserve and protect images of all known affected information systems and all relevant monitoring/packet capture data for at least 90 days from reporting the cyber incident to enable SDA to assess the cyber incident. Seller agrees to rapidly implement security measures as recommended by SDA consistent with Performer's Government approved security systems and to provide to SDA any additionally requested information to help the Parties resolve the cyber incident and to prevent future cyber incidents.

D. Public Release

All information and data covered by this Article must be reviewed and approved by SDA prior to any public release by the Provider. Submit any requests for review of information or data intended for public release to the SDA Strategic Engagement Cell.

E. Lower Tier Agreements
Seller shall include this Article in all subcontracts or lower tier agreements, regardless of tier, for work performed in support of this Agreement.
F. Definitions applicable to this clause
Compromise: 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.
Controlled Technical Information (CTI): 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.
Controlled Unclassified Information (CUI): Unclassified information that requires safeguarding or dissemination controls, pursuant to and consistent with applicable law, regulations, and Government-wide policies. Instructions for the use, marking, dissemination, and storage of CUI can be found in DoD Instruction 5200.48, "Controlled Unclassified Information (CUI)."
Cyber Incident: 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.
Information System: A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
Rapidly Report: Report to SDA within 72 hours of discovery of any cyber incident.

ARTICLE IX: ASSOCIATE CONTRACTOR AGREEMENT

A. Applicability
A similar clause or article will be included in all awards made against SDA Tranche 2 (T2) solicitations. Contractors or Performers receiving an award under a T2 solicitation will be required to enter into an Associate Contractor Agreement (ACA) with all of the prime awardees from the T2 solicitations.
B. ACA Language
The text of the ACA is as follows:
"It is recognized that the success of the SDA Tranche 2 of the Proliferated Warfighter Space Architecture (PWSA) depends in part upon the open exchange of information between the various Associate Contractors involved in the Tranche 2 PWSA effort. This article is intended to ensure appropriate

• Maintenance of a close liaison and working relationship

• Maintenance of a free and open information network with all Government-identified Associate Contractors

• Delineation of detailed interface responsibilities

• Entering into a written agreement with the other Associate Contractors setting forth the substance and procedures relating to the foregoing, and promptly providing the Procuring Contracting Officer or Agreements Officer with a copy of same

• Receipt of proprietary information from the Associate Contractors and transmittal of Contractor proprietary information to the Associate Contractors subject to any applicable proprietary information exchange agreements between Associate Contractors when, in either case, those actions are necessary for the performance of either"

coordination and integration of work by the Associate Contractors to achieve complete compatibility and to prevent unnecessary duplication of effort. By executing this agreement, the Contractor assumes the responsibilities of an Associate Contractor. For the purpose of this clause, the term Contractor includes subsidiaries, affiliates, and organizations under the control of the contractor (e.g., subcontractors).
Work under this agreement may involve access to proprietary or confidential data from an Associate Contractor. To the extent that such data is received by Seller from any Associate Contractor for the performance of this contract, Seller hereby agrees that any proprietary information received shall remain the property of the Associate Contractor and shall be used solely for the purpose of the SDA Tranche 2 Tracking Layer effort.
Information which is received from another Associate Contractor in writing or electronically and which is clearly identified as proprietary or confidential shall be protected in accordance with this provision. The obligation to retain such information in confidence will be satisfied if the Associate Contractor receiving such information utilizes the same controls as it employs to avoid disclosure, publication, or dissemination of its own proprietary information. The receiving Associate Contractor agrees to hold such information in confidence as provided herein so long as such information is of a proprietary/confidential or Limited Rights nature.
Seller hereby agrees to closely cooperate as an Associate Contractor with the other Associate Contractors on this effort. This involves as a minimum:

C. ACA Execution

Seller shall furnish copies of all ACAs to the AO immediately upon execution of the agreements. In the event that Seller and the Associate Contractor(s) are unable to reach an agreement, or if the technical data identified is not provided as scheduled, Seller shall promptly notify the SDA Program Manager and Contracting or Agreements Officer. The Government will determine the appropriate corrective action and will issue guidance to the affected Contractor.

D. ACA Subcontracts

Seller agrees to insert in all subcontracts hereunder which require access to proprietary information belonging to the Associate Contractors a provision which shall conform substantially to the language of this clause, including this paragraph.

ARTICLE X: PROHIBITION ON A BYTEDANCE COVERED APPLICATION

(a) Definitions. As used in this Article—

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 or performer under a contract or agreement 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 or performer incidental to a Federal contract or agreement.
(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 Performer 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 Performer under this agreement, including equipment provided by the Performer's employees; however, this prohibition does not apply if the Agreements Officer provides written notification to the Performer that an exception has been granted in accordance with OMB Memorandum M-23-13.
(c) Subcontracts or Sub-agreements. The Performer shall insert the substance of this article, including this paragraph (c), in all subcontracts or sub-agreements, including subcontracts or sub-agreements for the acquisition of commercial products or commercial services.