FIELD
AEROSPACE

ASES, LLC d/b/a Field Aerospace
6015 S. Portland Avenue
Oklahoma City, OK 73159
405-219-3400

Customer Required Flowdown Provisions for Items/Services Under Contract 2022-DARPA-0079

Supplement 406

Additional Clauses

1. ARTICLE V: SAFEGUARDING DARPA CONTROLLED UNCLASSIFIED INFORMATION AND CONTROLLED TECHNICAL INFORMATION AND CYBER INCIDENT REPORTING

A. Background

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

B. Safeguarding DARPA CUI and CTI

The Subcontractor 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 Agreement Officer for DARPA CUI and CTI that resides on the Subcontractor's information systems. Consistent with NIST SP 800-171, implementation may be tailored to facilitate equivalent safeguarding measures used in the Subcontractor systems and organization. Any suspected loss or compromise of DARPA CUI or CTI that resides on the Subcontractor's information systems shall be considered a cyber incident and require the Subcontractor to rapidly report the incident to DARPA in accordance with paragraph C below.

C. Cyber Incident Reporting

Upon discovery of a cyber incident involving DARPA CUI or CTI, the Subcontractor shall take immediate steps to mitigate any further loss or compromise. The Subcontractor shall rapidly report the incident to DARPA and provide sufficient details of the event—including identification of detected and isolated malicious software—to enable DARPA to assess the situation and provide feedback to the Subcontractor regarding further reporting and potential mitigation actions. The Subcontractor 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 DARPA to assess the cyber incident. The Subcontractor agrees to rapidly implement security measures as recommended by DARPA and to provide to DARPA 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 DARPA prior to any public release. The DARPA public release process is governed by DARPA Instruction 65. An online form is available to support those requests at:
https://www.darpa.mil/attachments/PublicReleaseSubmissionForm10232020.pdf

E. Lower Tier Agreements

The Subcontractor shall include this Article in all subcontracts or lower tier agreements, regardless of tier, for work performed in support of this Agreement.

F. Definitions

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 DARPA within 72 hours of discovery of any cyber incident.

2. ARTICLE XII: PROHIBITION ON TRANSACTIONS FOR CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT

(a) Definitions. As used in this Article—

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

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

Covered telecommunications equipment or services means—

(1) Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities);

(2) For the purpose of public safety, security of Government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities);

(3) Telecommunications or video surveillance services provided by such entities or using such equipment; or

(4) Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country.

Critical technology means—

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

(2) Items included on the Commerce Control List set forth in Supplement No. 1 to part 774 of the Export Administration Regulations under subchapter C of chapter VII of title 15, Code of Federal Regulations, and controlled—

(i) Pursuant to multilateral regimes, including for reasons relating to national security, chemical and biological weapons proliferation, nuclear nonproliferation, or missile technology; or

(ii) For reasons relating to regional stability or surreptitious listening;

(3) Specially designed and prepared nuclear equipment, parts and components, materials, software, and technology covered by part 810 of title 10, Code of Federal Regulations (relating to assistance to foreign atomic energy activities);

(4) Nuclear facilities, equipment, and material covered by part 110 of title 10, Code of Federal Regulations (relating to export and import of nuclear equipment and material);

(5) Select agents and toxins covered by part 331 of title 7, Code of Federal Regulations, part 121 of title 9 of such Code, or part 73 of title 42 of such Code; or

(6) Emerging and foundational technologies controlled pursuant to section 1758 of the Export Control Reform Act of 2018 (50 U.S.C. 4817).

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

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

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

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

(b) Prohibition.

(1) Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2019, from procuring or obtaining, or extending or renewing a contract (to include this Agreement) to procure or obtain, any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. The Subcontractor is prohibited from providing to the Government any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception at paragraph (c) of this Article applies or the covered telecommunication equipment or services are covered by a waiver described in FAR 4.2104.

(2) Reserved

(c) Exceptions. This Article does not prohibit Subcontractors from providing—

(1) A service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

(2) Telecommunications equipment that cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(d) Reporting requirement.

(1) In the event the Subcontractor identifies covered telecommunications equipment or services used as a substantial or essential component of any system, or as critical technology as part of any system, during contract (to include this Agreement) performance, or the Subcontractor is notified of such by a sub-awardee at any tier or by any other source, the Subcontractor shall report the information in paragraph (d)(2) of this Article to the Agreements Officer, unless elsewhere in this Agreement are established procedures for reporting the information; in the case of the Department of Defense, the Subcontractor shall report to the website at https://dibnet.dod.mil.

(2) The Subcontractor shall report the following information pursuant to paragraph (d)(1) of this Article:

(i) Within one business day from the date of such identification or notification: The Agreement number; the order number(s), if applicable; supplier name; supplier unique entity identifier (if known); supplier Commercial and Government Entity (CAGE) code (if known); brand; model number (original equipment manufacturer number, manufacturer part number, or wholesaler number); item description; and any readily available information about mitigation actions undertaken or recommended.

(ii) Within 10 business days of submitting the information in paragraph (d)(2)(i) of this Article: Any further available information about mitigation actions undertaken or recommended. In addition, the Subcontractor shall describe the efforts it undertook to prevent use or submission of covered telecommunications equipment or services, and any additional efforts that will be incorporated to prevent future use or submission of covered telecommunications equipment or services.

(e) Subcontracts. The Subcontractor shall insert the substance of this Article, including this paragraph (e) in all sub-awards and other contractual instruments, including sub-awards for the acquisition of commercial items.