1. NIST/ 7012

15. Safeguarding Covered Defense Information and Cyber Incident Reporting

The protection of Controlled Unclassified Information (CUI) while residing in nonfederal information systems and organizations is of paramount importance to federal agencies and can directly impact the ability of the federal government to successfully carry out its designated missions and business operations.

National Institute of Standards & Technology (NIST) Special Publication (SP) 800-171 provides federal agencies with recommended requirements for protecting the confidentiality of CUI: (i) when the CUI is resident in nonfederal information systems and organizations; (ii) when the information systems where the CUI resides are not used or operated by contractors of federal agencies or other organizations on behalf of those agencies; and (iii) where there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or government-wide policy for the CUI category or subcategory listed in the CUI Registry. The requirements apply to all components of nonfederal information systems and organizations that process, store, or transmit CUI, or provide security protection for such components. The CUI requirements are intended for use by federal agencies in contractual vehicles or other agreements established between those agencies and nonfederal organizations.

The Department of Defense (DOD) utilizes 48 CFR 252.204-7012 to direct the safeguarding of information and reporting of cybersecurity incidents for the DOD. Therefore, the guidance and requirements of 48 CFR 252.204-7012 as prescribed by 48 CFR 204.7304(c) are incorporated into this Agreement and shall flow-down to all Project Orders for non-COTS items, with all mention of Contractor understood to mean both the CMF and any Consortium Member awarded a Prototype Project, and all mention of Contracting Officer understood to mean Agreements Officer. 48 CFR 252.204-7012 shall not apply to COTS items. Each Project Order will identify the information that requires safeguarding and dissemination control.

2. 889 Covered Telecommunications Clause (please inform if you have the standard language from FAR 52.204-25 or CFR)

16. Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment

As appropriate, replace “Contractor” with “Consortium Member” or “MSTIC Member” and “contract” with “Agreement” or “Prototype Project”.

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

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 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 Contractor 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 clause applies or the covered telecommunication equipment or services are covered by a waiver described in FAR 4.2104.

(2) Section 889(a)(1)(B) 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, 2020, from entering into a contract, or extending or renewing a contract, with an entity that uses 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 clause applies or the covered telecommunication equipment or services are covered by a waiver described in FAR 4.2104. This prohibition applies to the use of covered telecommunications equipment or services, regardless of whether that use is in performance of work under a Federal contract.

(c) *Exceptions.* This clause does not prohibit contractors 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 Contractor 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 performance, or the Contractor is notified of such by a subcontractor at any tier or by any other source, the Contractor shall report the information in paragraph (d)(2) of this clause to the Contracting Officer, unless elsewhere in this contract are established procedures for reporting the information; in the case of the Department of Defense, the Contractor shall report to the website at https://dibnet.dod.mil. For indefinite delivery contracts, the Contractor shall report to the Contracting Officer for the indefinite delivery contract and the Contracting Officer(s) for any affected order or, in the case of the Department of Defense, identify both the indefinite delivery contract and any affected orders in the report provided at https://dibnet.dod.mil.

(2) The Contractor shall report the following information pursuant to paragraph (d)(1) of this clause

(i) Within one business day from the date of such identification or notification: the contract 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 clause: any further available information about mitigation actions undertaken or recommended. In addition, the Contractor 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) Contractor shall insert the substance of this clause, including this paragraph (e) and excluding

paragraph (b)(2), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items.

3. The following Clauses from MISTIC Base Agreement, M00_2023-369-000, dated 6/23/2023:

Article 3 - Limitation of Liability

(a) For the purposes of this Article, “Parties” means the CMF, the Consortium Member, and the Government where collectively identified, and “Party” where each entity is individually identified.

(b) With regard to the activities undertaken pursuant to this Agreement, no Party shall make any claim against the other, employees of the other, the others’ related entities (e.g., Contractors, Subcontractors), or employees of the others’ related entities for any injury to, or death of, its own employees or employees of its related entities, or for damage to, or loss of its own property, or that of its related entities, whether such injury, death, damage, or loss arises through negligence or otherwise, except in the case of willful misconduct.

(c) In no event, shall either Party be liable to each other for consequential, punitive, special, and incidental damages or other indirect damages, whether arising in contract (including warranty), tort (whether or not arising from the negligence of a Party), or otherwise, except to the extent such damages are caused by a Party's willful misconduct.

(d) Extension of Waiver of Liability. The Project Performer agrees to extend the limitation of liability as set forth above to sub-agreement holders at any tier performing Prototype Projects under this Agreement by requiring them, by contract or otherwise, to agree to waive all claims against the Parties to this Agreement.

Article 7 - Compliance with Laws Unique to Government Procurement

Each Consortium Member awarded a Prototype Project agrees and is required to comply with, 31 U.S.C. § 1352 relating to limitations on the use of appropriated funds to influence certain Federal contracts; 18 U.S.C. § 431 relating to officials not to benefit; 41 U.S.C. chapter 87, Kickbacks; 41 U.S.C. § 4712 and 10 U.S.C. § 2409 relating to whistleblower protections; 41 U.S.C. chapter 21 relating to procurement integrity; and 22 U.S.C. Chapter 78 relating to Combating Trafficking in Persons

Article 8 - Disclosure of Information

(c) MSTIC Members agree to include a similar requirement, including this paragraph (c), in each sub-agreement under any Prototype Project. Sub-agreement holders shall submit requests for authorization to release through the MSTIC Member to the AO via ATI.

Article 12 Export Control

(a) ATI and MSTIC Members shall comply with the International Traffic in Arms Regulation (22 CFR pt. 121 et seq.), the DoD Industrial Security Regulation (DoD 5220.22-R) and the Department of Commerce Export Regulation (15 CFR pt. 770 et seq.).

(b) ATI and MSTIC Members shall include and enforce inclusion of Export Control requirements as indicated in this paragraph, suitably modified to identify the appropriate parties, in all sub-agreements, regardless of tier, for developmental prototype work.