

RESOLUTION NUMBER 7813

WHEREAS, on or about February 15, 2017, the Beatrice Airport Authority, now the City of Beatrice, Nebraska ("City"), entered into Lease Agreement No. DTFACN-16-L-00196 with the United States of America, Federal Aviation Administration ("FAA") whereby the City leased the following described property to the FAA:

Approximately 200 square feet (10' x 20') of space located in the engine generator vault, located in Building 8, together with the rights for mounting RCO tilt-over antenna mast south of the facility, located at the Beatrice Municipal Airport; and

WHEREAS, said Lease expires on September 30, 2026; and

WHEREAS, the City and FAA desire to extend the term of said Lease for an additional ten (10) year period, beginning on October 1, 2026 and ending on September 30, 2036; and

WHEREAS, the City desires to execute Supplemental Agreement No. 1 to FAA Contract No. DTFACN-16-L-00196 to extend the term of said Lease and add additional provisions regarding prohibition of certain telecommunications and video surveillance services or equipment and security provisions for the protection of sensitive information in possession of the FAA.

NOW, THEREFORE, BE IT RESOLVED BY THE MAYOR AND CITY COUNCIL OF THE CITY OF BEATRICE, NEBRASKA:

SECTION 1. That the Mayor and City Clerk are hereby authorized to execute the Supplemental Agreement No. 1 to FAA Contract No. DTFACN-16-L-00196 to extend the term of said Lease and add additional provisions regarding prohibition of certain telecommunications and video surveillance services or equipment and security provisions for the protection of sensitive information in possession of the FAA. A copy of said Agreement is attached hereto as Exhibit "A" and is incorporated herein by reference.

SECTION 2. That Resolution Number 7784 and all resolutions or parts of resolutions in conflict herewith are hereby repealed.

RESOLUTION PASSED AND ADOPTED this 6th day of July, 2026.

Attest:



Erin Saathoff, MMC, City Clerk



Robert Morgan, Mayor

Exhibit "A"

<p>U.S. Department of Transportation Federal Aviation Administration</p> <p>SUPPLEMENTAL AGREEMENT</p>	<p>SUPPLEMENTAL AGREEMENT NO. 1 TO FAA CONTRACT NO. DTFACN-16-L-00196</p>
<p>DESCRIPTION or ADDRESS OF PREMISES: ATID/FC: BIE /RCO BEATRICE, NEBRASKA</p> <p>PREMISES: 200 square feet (10' x 20') of space located in the engine generator vault, located in Building 8, together with the rights for mounting the RCO tilt-over antenna mast south of the facility, located at Beatrice Municipal Airport.</p>	
<p>THIS AGREEMENT, made and entered into this date by and between THE CITY OF BEATRICE hereinafter called Lessor or Contractor, and the UNITED STATES OF AMERICA, Federal Aviation Administration, hereinafter called the FAA or Government:</p> <p>WHEREAS, on February 15, 2017, the parties entered Lease No. DTFACN-16-L-00196 for consideration and purpose more particularly stated in said contract; and,</p> <p>WHEREAS, said lease expires on September 30, 2026, and the Government has a continuing need to occupy the leased premises; and</p> <p>WHEREAS the Government desires to extend the term for an additional ten (10) year period, beginning October 1, 2026, through September 30, 2036, the Government shall pay the Lessor no monetary consideration; and</p> <p>WHEREAS, the Government has a requirement to add three (3) new clauses regarding prohibition of certain telecommunications and video surveillance services or equipment. Lessor confirms the applicable Representations; and</p> <p>WHEREAS, the Government has a requirement to add three (3) new security clauses as protection for sensitive information in possession of FAA that Lessor does not provide or use source prohibited in applicable FASCSA orders; and</p> <p>WHEREAS, the parties hereto desire to amend the above Contract, effective as of October 1, 2026.</p>	
<p>NOW THEREFORE, these parties for the considerations hereinafter mentioned covenant and agree that said real estate contract is amended, as follows:</p> <p>AMEND - PREAMBLE and TERM and replace it with the following:</p> <p>PREAMBLE (09/2021) – This lease is entered into by and between CITY OF BEATRICE , whose address is P.O. Box 277, Beatrice, NE 68310, and whose interest in the property hereinafter described is that of owner, hereby referred to as Lessor, and the United States of America, hereinafter referred to as the Government or the Federal Aviation Administration (FAA). WITNESSETH: The parties hereto, and for the consideration hereinafter mentioned, covenant and agrees as follows:</p> <p>TERM (08/02) To have and to hold said premises for the term commencing on February 15, 2017, and continues through September 30, 2036, inclusive</p>	

Add under 7. GENERAL CLAUSES the following:

Attachment A -NDAA Articles 6.9.5, 6.9.5-1 and 6.9.5-2 attached hereto and made a part hereof.

Attachment B – DCIP Article 6.9.6 and FASCSA Articles 6.9.8 and 6.9.8-1 attached hereto and made a part hereof.

All other terms and conditions of the real estate contract shall remain in full force and effect.

Lessor is required to sign this document and return One (1) Electronic copy to the issuing office.

IN WITNESS WHEREOF, the parties subscribed their names and date.

Lessor

THE CITY OF BEATRICE



Signature

7-6-26
Date

UNITED STATES OF AMERICA

Inger T. Brown
Real Estate Contracting Officer

Date

ATTACHMENT A

1. **Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment (07/2023) 6.9.5**

(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 AMS T3.8.9C.1.c(5).

(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 AMS T3.8.9C.1.c(5). This prohibition applies to an entity that uses covered telecommunications equipment or services, including use not in support of the Government.

(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 must 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. For indefinite delivery contracts, the Contractor must report to the Contracting Officer for the indefinite delivery contract and the Contracting Officer(s) for any affected order.

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

2. **Covered Telecommunications Equipment or Services- Representations (09/2021) 6.9.5-1 (a)**

Definitions. As used in this provision, "covered telecommunications equipment or services" has the meaning per the "Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment" clause in this contract.

(b) Procedures. The offeror must review the list of excluded parties in the System for Award Management (SAM) (<https://www.sam.gov>) for entities excluded from receiving federal awards for covered telecommunications equipment or services.

(c) Representations.

1. The offeror represents that it _____ does, _____ does not **provide** covered telecommunications equipment or services as part of its offered products or services to the Government in the performance of any contract, subcontract, or other contractual instrument.

2. After conducting a reasonable inquiry for purposes of this representation, the offeror represents that it _____ does, _____ does not **use** covered telecommunications equipment or services, or any equipment, system, or service that uses telecommunications equipment or services.

3. **Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment (09/2021) 6.9.5-2**

NOTE: The offeror must not complete the representation at paragraph (d)(1) in this provision if the offeror has represented that it does not provide covered telecommunications equipment or services as part of its offered products or services to the Government in the performance of any contract, subcontract, or other contractual instrument in the provision "Covered Telecommunications Equipment or Services – Representation" (c)(1). Additionally, The offeror must not complete the representation at paragraph (d)(2) in this provision if the offeror has represented that it does not use covered telecommunications equipment or services, or any equipment, system, or service that uses telecommunications equipment or services in the provision "Covered Telecommunications Equipment or Services – Representation" (c)(2).

PROVISION/CLAUSE:

(a) Definitions. As used in this provision--

Backhaul, covered telecommunications equipment or services, critical technology, interconnection arrangements, reasonable inquiry, roaming, and substantial or essential component have the meanings provided in the clause AMS clause 6.9.5, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment.

(b) Prohibitions.

(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.

Nothing in this prohibition will be construed to—

(i) Prohibit the head of the agency from procuring with an entity to provide a service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

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

(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 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 part of any system or as critical technology as part of any system. This prohibition applies to any entity that uses covered telecommunications equipment or services, including uses not in support of the Government.

Nothing in this prohibition will be construed to-

(i) Prohibit the head of the agency from procuring with an entity to provide a service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

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

(c) Procedures: The offeror must review the list of excluded parties in the System for Award Management (SAM) (<https://www.sam.gov>) for entities excluded from Federal awards for covered telecommunications equipment or services.

(d) Representations.

(1) The Offeror represents that it [] will, [] will not provide covered telecommunications equipment or services to the Government in the performance of any contract, subcontract or other contractual instrument resulting from this solicitation.

(2) After conducting a reasonable inquiry for purposes of this representation, the Offeror represents that that it [] does, [] does not USE covered telecommunications equipment or services, or use any equipment, system, or service that uses covered telecommunications equipment or services. The Offeror must provide the additional disclosure information required at paragraph (e) if the Offeror indicates “does”.

(e) Disclosures. Disclosure for the representation in paragraph (d) (1) of this provision-

If the Offeror has responded “will” in the representation in paragraph (d) (1) of this provision, the Offeror must provide the following information as part of the offer—

(1) For covered equipment

(i) The entity that produced the covered telecommunications equipment (include entity name, unique entity identifier, CAGE code, and whether the entity was the original equipment manufacturer (OEM) or a distributor, if known;

(ii) A description of all covered telecommunications equipment offered (include brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); and

(iii) Explanation of the proposed use of covered telecommunications equipment and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b) (1) of this provision;

(2) For covered services-

- (i) If the service is related to item maintenance, a description of all covered telecommunications services offered (include on the item being maintained: brand, model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); or
- (ii) If not associated with maintenance, the Product Service Code (PSC) of the service being provided; and explanation of the proposed uses of covered telecommunications services and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b)(1) of this provision. Disclosure for representation in paragraph (d) (2) of this provision. If the Offeror has responded “does” to paragraph (d)(2) of this provision, the offeror must provide the following information as part of the offer—

(3) For covered equipment

- (i) The entity that produced the covered telecommunications equipment (include entity name, unique entity identifier, CAGE code, and whether the entity was the OEM or a distributor, if known);
- (ii) A description of all covered telecommunications equipment offered (include brand; model number, such as original equipment manufacturer (OEM) number, manufacturer part number, or wholesaler number; and item description, as applicable); and
- (iii) Explanation of the proposed use of covered telecommunications equipment and services and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b) (2) of this provision.

(4) For covered services-

- (i) If the service is related to item maintenance, a description of all covered telecommunications services offered (include on the item being maintained: brand, model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); or
- (ii) If not associated with maintenance, the Product Service Code (PSC) of the service being provided; and explanation of the proposed uses of covered telecommunications services and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b)(2) of this provision.

ATTACHMENT B

1. **Cooperation with Defensive Counterintelligence Program Requirements (DCIP) (09/2021) 6.9.6**
 - a. The FAA's Defensive Counterintelligence Program (DCIP) (AXI-310) detects, deters, and denies illicit human and technical intelligence collection activities as well as addressing other national security concerns. Such activities and concerns include, but are not limited to, activities conducted by, on behalf of, or otherwise supporting, foreign governments or elements thereof; entities or individuals that meet the definition of "foreign power" or "agent of a foreign power" in 50 U.S.C. § 1801; foreign organizations; foreign persons; international terrorist organizations or activities; or agents of any of the foregoing; or any other individuals or entities acting on behalf of, or otherwise in support of, any of the foregoing, against the FAA, its employees, facilities, equipment, systems, networks, operations, and information.
 - b. Consistent with FAA Order 1600.84 FAA Defensive Counterintelligence Program, the contractor is required to cooperate to the fullest extent possible in the following requirements:
 - 1) Any authorized DCIP inquiry or Counterintelligence (CI) investigation connected with this contract requested by the FAA Office of Security and Hazardous Materials Safety (ASH) to include granting authorized ASH or outside investigative department or agency personnel access to contract information, records or contractor personnel;
 - 2) All applicable FAA security requirements as required under the contract consistent with FAA policy and applicable Federal law;
 - 3) When requested by the DCIP, and necessary to protect Controlled National Security Information (CNSI), Sensitive Unclassified Information (SUI), or otherwise protected information, contractor employees must sign a Defensive Counterintelligence Program Non-Disclosure Agreement (NDA) prior to being briefed on any information pertaining to a DCIP inquiry, CI investigation by another Department or Agency, or any other matter related to the DCIP. The NDA is located in Appendix C of the Order and in AMS Procurement Forms. Contractor employees are exempt from acknowledging any language in the NDA associated with unauthorized disclosure of received information that subjects FAA employees to personnel actions specified in the Human Resources Policy Manual (HRPM) Volume 4: Employee Relations ER-4.1 (4) and applicable collective bargaining agreements.
 - 4) Contractors must first coordinate with the DCIP at ASH-CI-Notify@faa.gov before contacting any law enforcement or investigative agencies on any known or suspected counterintelligence or other national security concern described in Paragraph 1 of FAA Order 1600.84.
 - 5) Contractors must notify the DCIP as soon as possible if any law enforcement or investigative agency contacts them directly on any matter covered by FAA Order 1600.84. If an employee receives a direct request from an outside law enforcement or investigative agency for evidence related to a counterintelligence or other national security concern as described in Paragraph 1 of FAA Order 1600.84, the employee will refer the law enforcement or investigative agency to AXI-310.
 - 6) Contractors must immediately notify the DCIP at ASH-CI-Notify@faa.gov, and the CO or their designee if their employees observe any of the following-
 - a) Suspected or known acts of foreign intelligence collection activity against the FAA or its employees, systems, networks, operations, facilities, equipment, or information;
 - b) Suspected or known espionage (See Appendix A of FAA Order 1600.84 for definition);
 - c) Suspected or known unauthorized disclosure of CNSI, SUI, or otherwise protected information in the possession of the FAA by a FAA employee to a foreign government or element thereof, a foreign organization, an entity or individual that meets the definition of "foreign power" or "agent of a foreign power" in 50 U.S.C. § 1801, a foreign person, an international terrorist organization or activity, an agent of any of the foregoing, or any other individual or entity acting on behalf of or otherwise supporting any of the foregoing; or
 - d) Suspected or known theft, unauthorized disclosure, or unauthorized amassing of CNSI, SUI, or otherwise

protected information in the possession of the FAA known or suspected to be for the purpose of conveying it to a foreign government or element thereof, an entity or individual that meets the definition of “foreign power” or “agent of a foreign power” in 50 U.S.C. § 1801, a foreign organization, a foreign person, an international terrorist organization or activity, an agent of any of the foregoing, any other individual or entity acting on behalf of or otherwise supporting any of the foregoing, or an unknown recipient, or statements of intent by an FAA employee to engage in any such actions. SUI or otherwise protected unclassified information whose theft, unauthorized disclosure, or unauthorized amassing, for the purposes described in the preceding sentence, is of concern includes, but is not limited to:

- i. Non-public information from an official FAA data network or information;
- ii. Imagery;
- iii. Technical specifications;
- iv. Trade secrets;
- v. Proprietary information;
- vi. Sensitive Security Information (SSI); and
- vii. Any other SUI

e) Activities similar to those described in paragraphs b(6)(a)-(d) by, on behalf of, or otherwise supporting, potential lone wolf actors, malicious insiders, or transnational organizations of a national security concern.

If notification of the CO or their designee is not feasible owing to the CO and/or their designee being one of the suspicious actor(s), the contractor must notify the DCIP directly at the above email address if they observe any of the above activities.

7) Elicitation attempts. Elicitation is the strategic use of conversation to extract information from people without giving them the feeling they are being interrogated. It is a technique used to discreetly gather information. It is a conversation with a specific purpose: collect information that is not readily available and do so without raising suspicion that specific facts are being sought. The conversation can be in person, over the phone, or in writing.

Contractors must immediately notify the DCIP at ASH-CI-Notify@faa.gov, and the CO and/or their designee if their employees experience any known or suspected direct (e.g., personal encounter or telephone) or indirect (e.g., electronic or written communication) elicitation or attempted elicitation of CNSI, SUI, or otherwise protected information in the possession of the FAA by any suspicious entity or person, regardless of ethnicity, nationality, or FAA employment status, as soon as possible, but no later than 12 hours after the time of the incident, initial detection, or receipt of report, as applicable, or the next business day if the incident, initial detection, or receipt of report, as applicable, occurs on a weekend or holiday. Contractors must report these incidents regardless of where, when, or how the contact took place, or whether the employee was on or off duty. Suspicious activities include, but are not limited to:

- a) Direct or indirect contact or communication with a known or suspected foreign or foreign-affiliated person, or an unknown or unfamiliar person, seeking access to or disclosure of any CNSI, SUI, or otherwise protected information in the possession of the FAA for which such person does not meet the applicable access requirements, or that is outside the scope of their official duties;
- b) Direct or indirect contact or communication with a known or suspected foreign or foreign-affiliated person, or an unknown or unfamiliar person, seeking specific information about an FAA employee’s official duty responsibilities, work projects, access to information, security clearance, travel plans, coworkers’ identities, or Information Technology (IT) system credentials for which such person does not meet the applicable access requirements, or that is outside the scope of their official duties;
- c) Direct or indirect contact, communication, or observance of a known or suspected foreign or foreign-affiliated person, or an unknown or unfamiliar person, seeking unauthorized access to FAA employees, equipment, operations, systems, information, facilities, or networks, including through a Personal Electronic Device (PED);
- d) Direct or indirect contact, communication, or observance of a known or suspected foreign or foreign-

affiliated person, or an unknown or unfamiliar person, introducing, or seeking to introduce, unauthorized digital media or software into any FAA equipment, facilities, systems, or networks, including through a PED;

- e) Offers of compensation, gifts, or favors in exchange for FAA information or access to such information, regardless of medium; or access to FAA employees, equipment, operations, facilities, systems, or networks;
- f) Threats, attempts to coerce, or attempts to exploit any FAA employee by a known or suspected foreign or foreign-affiliated person, or by an unknown or unfamiliar person, in order to illicitly acquire FAA information or access to FAA employees, equipment, operations, facilities, systems, information, or networks;
- g) Solicitation by any person of FAA information for which they do not meet the applicable access requirements or that is outside the scope of their official duties;
- h) A request by any person for access to FAA employees, facilities, equipment, operations, systems, information, or networks for which they do not meet the applicable access requirements or that is outside the scope of their official duties; and
- i) Suspicious or unexplained contact by any person with an FAA employee, where the person has suspicious or unexplained knowledge of the employee.

Unless requested by ASH, contractors must not disclose an elicitation attempt of the nature described above, in any other manner than to report the attempt to the CO or their designee and request that they report it to the DCIP. If that is not feasible, or if the CO or their designee are the suspicious actor(s), contractors may make these reports directly to the DCIP at the above email address. Contractors must not take any actions on their own initiative, as doing so may interfere with a DCIP inquiry or CI investigation.

- c. Failure to cooperate with any of the activities under section (b) above may be considered by the FAA to be a material breach of the contract.
- d. The Contractor is responsible for ensuring that the provisions of this clause flow down to its subsidiaries, subcontractors, and consultants performing this contract.

2. Federal Acquisition Supply Chain Security Act Orders—Representation and Disclosures (04/2024) 6.9.

(a) Definitions. As used in this provision, Covered article, FASCSA order, Intelligence community, National security system, Reasonable inquiry, Sensitive compartmented information, Sensitive compartmented information system, and Source have the meaning provided in the AMS Real Property Clause 6.9.8-1, Federal Acquisition Supply Chain Security Act Orders—Prohibition.

(b) Prohibition. Contractors are prohibited from providing or using as part of the performance of the contract any covered article, or any products or services produced or provided by a source, if the prohibition is set out in an applicable Federal Acquisition Supply Chain Security Act (FASCSA) order, as described in paragraph (b)(1) of AMS Real Property Clause 6.9.8-1, Federal Acquisition Supply Chain Security Act Orders—Prohibition.

(c) Procedures.

(1) The Offeror must search for applicable FASCSA orders of the type identified in paragraph (b)(1) of AMS Real Property Clause 6.9.8-1 in the System for Award Management (SAM). Issued FASCSA Orders may be identified by selecting the “View FASCSA Orders” button from the SAM homepage (<https://www.sam.gov>) and viewing or downloading FASCSA orders from the Supply Chain Security Orders webpage.

(2) The Offeror must review the SIR for any FASCSA orders that are not in SAM but are effective and do apply to the SIR and resultant contract (see AMS Guidance T3.8.9.C.4.c.(2)(A)(ii)).

(3) FASCSA orders issued after the publication date of the SIR do not apply unless the order is subsequently added to the SIR via amendment.

(d) Representation. By submission of this offer, the offeror represents that it has conducted a “reasonable inquiry” (as defined in AMS Real Property Clause 6.9.8-1), and that the offeror does not propose to provide or use in response to this SIR any covered article, or any products or services produced or provided by a source, if the covered article or the source is prohibited by an applicable FASCSCA order in effect on the date the SIR was issued, except as waived by the SIR, or as disclosed in paragraph (e) Disclosures, below.

(e) Disclosures. The purpose for this disclosure is so the FAA may decide whether to issue a waiver. For any covered article, or any products or services produced or provided by a source, if the covered article or the source is subject to an applicable FASCSCA order, and the Offeror is unable to represent compliance, then the Offeror must provide the following information as part of the offer:

- (1) Name of the product or service provided to the Government;
- (2) Name of the covered article or source subject to a FASCSCA order;
- (3) If applicable, name of the vendor, including the Commercial and Government Entity code and unique entity identifier (if known), that supplied the covered article or the product or service to the Offeror;
- (4) Brand;
- (5) Model number (original equipment manufacturer number, manufacturer part number, or wholesaler number);
- (6) Item description; and
- (7) Reason why the applicable covered article or the product or service is being provided or used.

(f) FAA review of disclosures. The Contracting Officer will review disclosures provided in paragraph (e) Disclosures, to determine if any waiver may be sought. A Contracting Officer may choose not to pursue a waiver for covered articles or sources otherwise subject to a FASCSCA order and may instead make an award to an offeror that does not require a waiver.

3. Federal Acquisition Supply Chain Security Act Orders—Prohibition (04/2024) 6.9.8-1 (a) Definitions.

As used in this clause—

Covered article, as defined in 41 U.S.C. 4713(k), means—

- (1) “Information technology,” as defined in 40 U.S.C. 11101, including cloud computing services of all types;
- (2) “Telecommunications equipment” or “telecommunications service,” as those terms are defined in section 3 of the Communications Act of 1934 (47 U.S.C. 153);
- (3) The processing of information on a Federal or non-Federal information system, subject to the requirements of the Controlled Unclassified Information program (see 32 CFR part 2002); or
- (4) Hardware, systems, devices, software, or services that include embedded or incidental information technology.

FASCSCA order means any of the following orders issued under the Federal Acquisition Supply Chain Security Act (FASCSCA) requiring the removal of covered articles from executive agency information systems or the exclusion of one or more named sources or named covered articles from executive agency procurement actions, as described in 41 CFR 201–1.303(d) and (e):

- (1) The Secretary of Homeland Security may issue FASCSCA orders applicable to civilian agencies, to the extent not covered by paragraph (2) or (3) of this definition. This type of FASCSCA order may be referred to as a Department of Homeland Security (DHS) FASCSCA order.
- (2) The Secretary of Defense may issue FASCSCA orders applicable to the Department of Defense (DoD) and national security systems other than sensitive compartmented information systems. This type of FASCSCA order may be referred to as a DoD FASCSCA order.
- (3) The Director of National Intelligence (DNI) may issue FASCSCA orders applicable to the intelligence

community and sensitive compartmented information systems, to the extent not covered by paragraph (2) of this definition. This type of FASCSA order may be referred to as a DNI FASCSA order.

Intelligence community, as defined by 50 U.S.C. 3003(4), means the following—

- (1) The Office of the Director of National Intelligence;
- (2) The Central Intelligence Agency;
- (3) The National Security Agency;
- (4) The Defense Intelligence Agency;
- (5) The National Geospatial-Intelligence Agency;
- (6) The National Reconnaissance Office;
- (7) Other offices within the Department of Defense for the collection of specialized national intelligence through reconnaissance programs;
- (8) The intelligence elements of the Army, the Navy, the Air Force, the Marine Corps, the Coast Guard, the Federal Bureau of Investigation, the Drug Enforcement Administration, and the Department of Energy;
- (9) The Bureau of Intelligence and Research of the Department of State;
- (10) The Office of Intelligence and Analysis of the Department of the Treasury;
- (11) The Office of Intelligence and Analysis of the Department of Homeland Security; or
- (12) Such other elements of any department or agency as may be designated by the President, or designated jointly by the Director of National Intelligence and the head of the department or agency concerned, as an element of the intelligence community.

National security system, as defined in 44 U.S.C. 3552, means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—

- (1) The function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions, but does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications); or
- (2) Is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

Reasonable Inquiry means an inquiry designed to uncover any information in the entity's possession about the identity of any covered articles, or any products or services produced or provided by a source. This applies when the covered article or the source is subject to an applicable FASCSA order. A reasonable inquiry excludes the need to include an internal or third-party audit.

Sensitive compartmented information means classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems established by the Director of National Intelligence.

Sensitive compartmented information system means a national security system authorized to process or store sensitive compartmented information.

Source means a non-Federal supplier, or potential supplier, of products or services, at any tier.

(b) Prohibition.

- (1) Unless an applicable waiver has been issued by the issuing official, Contractors are prohibited from providing or using as part of the performance of the contract any covered article, or any products or services produced or provided by a source, if the covered article or the source is prohibited by any applicable FASCSA orders identified by the checkbox(es) in this paragraph (b)(1).

Yes No DHS FASCSA orders

Yes No DoD FASCSCA orders

Yes No DNI FASCSCA orders

(2) The Contractor must search for applicable FASCSCA orders of the type identified in paragraph (b)(1) of this clause in the System for Award Management (SAM). Issued FASCSCA Orders may be identified by selecting the “View FASCSCA Orders” button from the SAM homepage (<https://www.sam.gov>) and viewing or downloading FASCSCA orders from the Supply Chain Security Orders webpage.

(3) The FAA may identify in the SIR additional FASCSCA orders that are not in SAM, which are effective and apply to the SIR and resultant contract.

(4) A FASCSCA order issued after the publication date of the SIR applies to this contract only if added by an amendment to the SIR or by modification to the contract. However, see paragraph (c) of this clause.

(5) Contractor request for waivers.

(i) Required disclosures. If the contractor wishes to ask for a waiver of the requirements of an existing order identified in a SIR or contract for a waiver of the requirements of a new FASCSCA order being applied through modification, then the Contractor must disclose the following:

(A) Name of the product or service provided to the Government;

(B) Name of the covered article or source subject to a FASCSCA order;

(C) If applicable, name of the vendor, including the Commercial and Government Entity code and unique entity identifier (if known), that supplied or supplies the covered article or the product or service to the Offeror;

(D) Brand;

(E) Model number (original equipment manufacturer number, manufacturer part number, or wholesaler number);

(F) Item Description;

(G) Reason why the applicable covered article or the product or service is being provided or used;

(ii) FAA review of disclosures. The Contracting Officer will review disclosures provided in paragraph (b)(5)(i) to determine if any waiver is warranted. A Contracting Officer may choose not to pursue a waiver for covered articles or sources otherwise covered by a FASCSCA order and to instead pursue other appropriate action.

(c) Notice and reporting requirement.

(1) During contract performance, the Contractor is required to:

(i) Comply with all FASCSCA orders identified under paragraph (b) of this clause; and

(ii) Review SAM.gov at least once every three months, or as advised by the Contracting Officer, to check for covered articles subject to FASCSCA order(s), or for products or services produced by a source subject to FASCSCA order(s) not currently identified under paragraph (b) of this clause.

(2) If the Contractor identifies a new FASCSCA order(s) that could impact their supply chain, then the Contractor must conduct a reasonable inquiry to identify whether a covered article or product or service produced or provided by a source subject to the FASCSCA order(s) was provided to the Government or used during contract performance.

(3) If the Contractor identifies, including through any notification by a subcontractor at any tier, that a covered article or product or service produced or provided by a covered source was provided to the Government or used during contract performance and is subject to a FASCSCA order(s) identified in paragraph (b) of this clause, or a new FASCSCA order identified in paragraph (c)(2) of this clause, the Contractor must submit a report to the Contracting Officer.

(4) The Contractor must report the following information for each covered article or each product or service produced or provided by a source, where the covered article or source is subject to a FASCSCA order, pursuant to paragraph (c) of this clause:

(i) Within 3 business days from the date of such identification or notification:

- (A) Contract number;
 - (B) Order number(s), if applicable;
 - (C) Name of the product or service provided to the Government or used during performance of the contract;
 - (D) Name of the covered article or source subject to a FASCSA order;
 - (E) If applicable, name of the vendor, including the Commercial and Government Entity code and unique entity identifier (if known), that supplied the covered article or the product or service to the Contractor;
 - (F) Brand;
 - (G) Model number (original equipment manufacturer number, manufacturer part number, or wholesaler number);
 - (H) Item description; and
 - (I) Any readily available information about mitigation actions undertaken or recommended.
- (ii) Within 10 business days of submitting the information in paragraph (c)(4)(i) of this clause:
- (A) Any further available information about mitigation actions undertaken or recommended.
 - (B) In addition, the Contractor must describe the efforts it undertook to prevent submission or use of the covered article or the product or service produced or provided by a source subject to an applicable FASCSA order, and any additional efforts that will be incorporated to prevent future submission or use of the covered article or the product or service produced or provided by a source that is subject to an applicable FASCSA order.
- (d) Removal. Upon notification from the contracting officer, during the performance of the contract, the Contractor must promptly make any necessary changes or modifications to remove any covered article or any product or service produced or provided by a source that is subject to an applicable Governmentwide FASCSA order.
- (e) Subcontracts.
- (1) The Contractor must insert the substance of this clause, including this paragraph (e) and excluding paragraph (c)(1) of this clause, in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial products and commercial services.
 - (2) The Government may identify in the SIR additional FASCSA orders that are not in SAM, which are effective and apply to the contract and any subcontracts and other contractual instruments under the contract. The Contractor or higher-tier subcontractor must notify their subcontractors, and suppliers under other contractual instruments, that the FASCSA orders in the SIR that are not in SAM apply to the contract and all subcontracts.



MEMORANDUM

TO: Mayor & City Council

DATE SUBMITTED: June 30, 2026

FROM: Erin Saathoff
City Clerk

FOR AGENDA OF: July 6, 2026

SUBJECT: Supplemental Agreement Revision

EXHIBIT(S): Resolution and Agreement

This item was approved at the May 4, 2026 Council meeting, however, upon review by the FAA it was discovered that the Supplemental Agreement that was signed contained incorrect term dates. To ensure the agreement accurately reflects the intended lease term, the FAA has asked that a corrected Supplemental Agreement 1 be executed.