U.S GOVERNMENT CONTRACT PROVISIONS FROM THE DEPARTMENT OF DEFENSE FEDERAL ACQUISITION SUPPLEMENT (DFARS)
TC002, Supplement 2

NOTE: These clauses are applicable to Purchase Orders or Subcontracts issued by Crestview Aerospace, LLC or Kemco Tool & Machine Company dba Kemco Aerospace in support of a U.S. Government Prime Contract.

1. When the materials or products furnished are for use in connection with a U. S. Government Department of Defense contract or subcontract, in addition to the General Provisions and the FAR provisions, the following provisions shall apply, as required by the terms of the prime contractor or by operation of law or regulation. In the event of a conflict between these DFARS provisions and the General Provisions or the FAR provisions, the DFARS provisions shall control**.** Clauses in this document may not be applicable to specific orders due to the type of subcontract/purchase order to be issued, dollar thresholds under requirements of the FAR, DFARS or Public Law or Mandatory Flow Down requirements of a particular prime contract. Clauses not applicable for these reasons shall not be removed from this document and will be considered by all parties to be without force and effect.

2. The following clauses set forth in the DFARS, in effect as of the date of the prime contract, are incorporated herein by reference with the same force and effect as if they were given in full text. In all clauses listed herein, the terms "Government," "Contracting Officer," and "Contractor" shall be revised to suitably identify the contracting parties under this purchase order and affect the proper intent of the provision, except where further clarified or modified below. "Subcontractor;" however, shall mean "Seller's Subcontractor" under this purchase order. The Seller, by signing its offer, hereby certifies compliance with the following clauses and is, therefore, eligible for award.

A. Title of Clause ..... DFARS

1. Requirement to Inform Employees of Whistleblower Rights..... 252.203.7002
   (a) The Contractor shall inform its employees in writing, in the predominant native language of the workforce, of contractor employee whistleblower rights and protections under 10 U.S.C. 2409, as described in subpart 203.9 of the Defense federal Acquisition Regulation Supplement. (b) The Contractor shall include the substance of this clause, including this paragraph
   (b), in all subcontracts. (End of Clause)
2. Disclosure of Information 252.204-7000
3. Alternate A, System For Award Management.....252.204-7004
4. Alternate A, Annual Representations and Certifications 252.204-7007
5. Limitations on the USE and Disclosure of Third Party Contractor Reported Cyber Incident Information 252.204-7009
6. Safeguarding Covered Defense Information and Cyber Incident Reporting and CDI will be flowed down to or processed by Seller 252.204-7012
7. Removed & Reserved by DFARS Case 2019-D021..... .....~~252.204-7013~~
8. Limitations on the Use or Disclosure of Information by Litigation Support Contractors..... ..252.204-7014
9. Disclosure of Information to Litigation Support Contractors.....252.204-7015
10. Disclosure of Ownership of Control by a Foreign Government 252.209-7002
11. Item Unique Identification and Valuation.....252.211-7003
12. Passive Radio Frequency Identification 252.211-7006
13. Reporting of Government Furnished Property 252.211-7007
14. Pricing Adjustments 252.215-7000
15. Cost Estimating System Requirements.....252.215-7002
16. Award Fee Reduction or Denial for Jeopardizing the Health and Safety of Gov't Personnel.....252.216-7004
17. Restrictions on Employment of Personnel 252.222-7000
18. Hazard Warning Labels (Fill in State where this purchase order will be performed.) 252.223-7001
19. Safety Precautions for Ammunition and Explosives 252.223-7002
20. Change in Place of Performance - Ammunition and Explosives 252.223-7003
21. Drug-Free Work Force 252.223-7004
22. Prohibition on Storage and Disposal of Toxic and Hazardous Materials 252.223-7006
23. Safeguarding Sensitive Conventional Arms, Ammunition and Explosives 252.223-7007
24. Prohibition of Hexavalent Chromium..... 252.223-7008
25. Buy American Act – Balance of Payments Program Certificate.....252.225-7000
26. Buy American Act and Balance of Payments Program 252.225-7001
27. Qualifying Country Sources as Subcontractors 252.225-7002
28. Prohibition on Acquisition of United States Munitions List Items from Communist Chinese Military Companies.....252.225-7007

77. Requirement for Competition Opportunity for American Steel Producers, Fabricators, and Manufacturers (for Construction Subcontracts) 252.236-7013
78. Training for Contract Personnel Interacting with Detainees 252.237-7019
79. Continuation of Essential Contractor Services 252.237-7023
80. Notice of Continuation of Essential Contractor Services 252.237-7024
81. Protection Against Compromising Emanations 252.239-7000
82. Information Assurance Contractor Training and Certification 252.239-7001
83. Cloud Computing Services 252.239-7010
84. Telecommunications Security Equipment, Devices, Techniques, and Services 252.239-7016
85. Notice of Supply Chain Risk 252.239-7017
86. Supply Chain Risk 252.239-7018
87. Pricing of Contract Modifications 252.243-7001
88. Subcontracts for Commercial Items and Commercial Components (DoD Contracts) 252.244-7000
89. Tagging, Labeling, and Marking Government Furnished Property 252.245-7001
90. Reporting Loss of Government Property 252.245-7002
91. Contractor Property Management System 252.245-7003
92. Reporting, Re-utilization and Disposal 252.245-7004
93. Material Inspection and Receiving Report 252.246-7000
94. Notification of Potential Safety Issues 252.246-7003
95. Safety of Facilities, Infrastructure, and Equipment for Military Operations 252-246-7004
96. Contractor Counterfeit Electronic Part Detection and Avoidance System 252.246-7007
97. Sources of Electronic Parts 252.246-7008
98. Pass-Through of Motor Carrier Fuel Surcharge Adjustment to the Cost Bearer 252.247-7003
99. ~~Notification of Transportation of Supplies by Sea~~ (RESERVED) 252.247-7024

B. ORDERS OVER THE SIMPLIFIED ACQUISITION THRESHOLD ALSO INCLUDE THE FOLLOWING:

1. Prohibition on Persons Convicted of Fraud or Other Defense–Contract-Related Felonies 252.203-7001
2. Removed and Reserved 252.209-7001
3. Subcontracting with Firms that are Owned or Controlled by the government of a Terrorist Country 252.209-7004
4. Requests for Equitable Adjustment 252.243-7002
5. Contractor Purchasing System Administration 252.244-7001
6. Representation of Extent of Transportation by Sea 252.247-7022
7. Transportation of Supplies by Sea 252.247-7023
8. ~~Notification of Transportation of Supplies by Sea~~ (RESERVED) 252.247-7024

C. ORDERS OVER $ 500,000 ALSO INCLUDE THE FOLLOWING:

1. Small Business Subcontracting Plan (DoD Contracts) - over $700K 252.219-7003
2. Report of Intended Performance Outside the United States – Submission with Offer ($700,000) 252-225-7003
3. Report of Intended Performance Outside the United States & Canada – Submission After Award ($700,000) 252.225-7004
4. Removed and Reserved 252.225-7006
5. Utilization of Indian Organizations, Indian-Owned Economic Enterprises, and Native Hawaiian Small Business Concerns 252.226-7001
6. Notification of Anticipated Contract Termination or Reduction 252.249-7002

D. ORDERS OVER $1,000,000 ALSO INCLUDE THE FOLLOWING:

1. Agency Office of the Inspector General ($5M) 252.203-7003
2. Display of Fraud Hotline Posters (Over $5.5M) 252.203-7004
3. Acquisition Streamlining 252.211-7000
4. Restriction on the Use of Mandatory Arbitration Agreements 252.222-7006

5. Report of Intended Performance Outside the United States & Canada – Submission with Offer (over $13.5 million) 252.225-7003
6. Waiver of United Kingdom Levies – Evaluation of Offers 252.225-7032
7. Waiver of United Kingdom Levies 252.225-7033

E. **ORDERS FOR MAJOR DEFENSE ACQUISITION PROGRAMS INCLUDE THE FOLLOWING:**

1. Notice of Prohibition Relating to Organizational Conflict of Interest – Major Defense Acquisition Program 252.209-7008
2. Organizational Conflict of Interest – Major Defense Acquisition Program 252.209-7009
3. Earned Value Management System (Orders over $50M)…….…… ..252.234-7002
4. Notice of Cost and Software Data reporting System (Orders over $50M) 252.234.7003
5. Cost and Software Date Reporting System (Orders over $50M) 252.234-7004

CERTIFICATIONS ***the Offeror, by signing its offer, hereby certifies compliance with the following clauses and is, therefore eligible for Award.***

1. Representation Regarding Combating Trafficking in Persons ……252.222-7007
2. Representation of Use of Cloud Computing 252.239-7009

U.S GOVERNMENT CONTRACT PROVISIONS FROM THE DEPARTMENT OF DEFENSE FEDERAL ACQUISITION SUPPLEMENT (DFARS)
TC002, Supplement 2

The following clauses are incorporated in full text and will be flowed to Suppliers at all tiers:

252.239-7018 Supply Chain Risk.
As prescribed in 239.7306(b), use the following clause: SUPPLY CHAIN RISK (OCT 2015)

(a) Definitions. As used in this clause–
"Information technology" (see 40 U.S.C 11101(6)) means, in lieu of the definition at FAR 2.1, any equipment, or interconnected system(s) or subsystem(s) of equipment, that is used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency.
(1) For purposes of this definition, equipment is used by an agency if the equipment is used by the agency directly or is used by a contractor under a contract with the agency that requires—
(i) Its use; or
(ii) To a significant extent, its use in the performance of a service or the furnishing of a product.
(2) The term "information technology" 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.
(3) The term "information technology" does not include any equipment acquired by a contractor incidental to a contract.
"Supply chain risk," means the risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a national security system (as that term is defined at 44 U.S.C. 3542(b)) so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system.
(b) The Contractor shall mitigate supply chain risk in the provision of supplies and services to the Government.
(c) In order to manage supply chain risk, the Government may use the authorities provided by section 806 of Public Law. 111-383. In exercising these authorities, the Government may consider information, public and non-public, including all-source intelligence, relating to a Contractor's supply chain.
(d) If the Government exercises the authority provided in section 806 of Pub. L. 111-383 to limit disclosure of information, no action undertaken by the Government under such authority shall be subject to review in a bid protest before the Government Accountability Office or in any Federal court.
(e) The Contractor shall include the substance of this clause, including this paragraph (e), in all subcontracts involving the development or delivery of any information technology, whether acquired as a service or as a supply.

(End of clause)

252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting. (Oct 2016)

(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 Government wide 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—
Noncommercial Items, 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 http://dx.doi.org/10.6028/NIST.SP.800-171) 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 non-applicable 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/resources/documents/) 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 http://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 http://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 http://iase.disa.mil/pki/eca/Pages/index.aspx.

(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 items, 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)