

**Supplemental Flow Down Requirements
S10892-S10893**

In addition to Buyer's terms and conditions of purchase, the following terms shall apply to purchase orders in support of the contracts referenced above. In the event of conflict between Buyer's terms and conditions of purchase and these terms, these terms shall take precedence.

1. STANDARDIZATION

- a) The U.S. Government has expressed a desire to procure up to twenty-six (26) cutters under the FRC PHASE II program. It is extremely important to the U.S. Government to maintain standardization within the FRC PHASE II fleet to minimize logistical cost for spare parts and training. Any changes to the equipment supplied under the FRC PHASE II program that differ from the first cutter must be approved in writing by BUYER. Any cost incurred by BUYER for changes proposed by SELLER shall be to SELLER's account. Changes shall include, but not be limited to, changes to the model number, components, parts, part numbers, technical data packages, software, firmware, hardware, VFI, or similar items.
- b) Standardization of all cutters under this Contract shall be in accordance with the requirements of this Contract unless otherwise approved by BUYER. All cutters constructed under this Contract shall have machinery and equipment which is identical in every respect except as authorized in writing by BUYER. If the SELLER considers that strict compliance with this requirement is impracticable as to any individual item of machinery or equipment or any component thereof, the SELLER shall notify BUYER immediately and shall propose alternatives to the requirement. Where the SELLER is permitted to deviate from contract requirements, BUYER will determine the effect, if any, of such approved deviation on the contract price and the contract shall be modified accordingly.
- c) The contractor shall be responsible for addressing Diminishing Manufacturing Sources/Material Shortages (DMSMS) and obsolescence throughout the life of the contract. A description of the approach to DMSMS/obsolescence shall be included in the SELLER's proposal. If DMSMS/obsolescence concerns appear to affect the equipment the SELLER is providing under this contract, the SELLER shall be responsible notifying BUYER as soon as practicable upon SELLER's discovery of the impending obsolescence and to recommend solutions which may include, but not be limited to, alternate vendors, substitute parts, or new sources of supply. Configuration management will also be considered as recommended solutions are developed and provided.
- d) The SELLER shall use sound procurement practices in furtherance of this standardization objective and shall include the substance of this clause and the specifications in subcontracts and purchase orders.
- e) While engaged in the efforts described above, the SELLER shall:
 - i. Inform BUYER if unable to arrange pricing agreements and indicate why; and
 - ii. Use best efforts to extend pricing agreements for other types of equipment to enhance standardization and supportability.

2. EXPORT CONTROL

- a) SELLER agrees to comply with all applicable U.S. export control laws and regulations, specifically including, but not limited to, the requirements of the Arms Export Control Act, 22 U.S.C. 2751-2794, including the International Traffic in Arms Regulation (ITAR), 22 C.F.R. 120 et seq.; and the Export Administration Act, 50 U.S.C. app. 2401-2420, including the Export Administration Regulations, 15 C.F.R. 730-774; including the requirement for obtaining any export license or agreement, if

applicable. Without limiting the foregoing, SELLER agrees that it will not transfer any export controlled item, data, or services, to include transfer to foreign persons employed by or associated with, or under contract to SELLER or SELLER'S lower-tier suppliers, without the authority of an export license, agreement, or applicable exemption or exception. Further, technical documents shall be marked with the appropriate ITAR control statements.

b) Definitions.

i. "Export-controlled items," as used in these Terms and Conditions, means items subject to the Export Administration Regulations (EAR) (15 C.F.R. Parts 730-774) or the International Traffic in Arms

Regulations (ITAR) (22 C.F.R. Parts 120-130). The term includes:

ii. "Defense items," defined in the Arms Export Control Act, 22 U.S.C. 2778 (j) (4) (A), as defense articles, defense services, and related technical data, and further defined in the ITAR, 22 C.F.R. Part 120.

iii. "Items," defined in the EAR as "commodities", "software", and "technology", are terms that are defined in the EAR, 15 C.F.R. 772.1.

c) SELLER agrees to notify BUYER if any deliverable under this Contract is restricted by export control laws or regulations.

d) SELLER shall immediately notify BUYER if SELLER is, or becomes, listed in any Denied Parties List or if SELLER'S export privileges are otherwise denied, suspended or revoked in whole or in part by any U.S. Government entity or agency.

e) If SELLER is engaged in the business of either exporting or manufacturing (whether exporting or not) defense articles or furnishing defense services, SELLER represents that it is registered with the Office of Defense Trade Controls, as required by the ITAR, and it maintains an effective export/import compliance program in accordance with the ITAR.

f) Where SELLER is a signatory under a BUYER export license or export agreement (e.g., TAA, MLA), SELLER shall provide prompt notification to BUYER in the event of changed circumstances including, but not limited to, ineligibility, a violation or potential violation of the ITAR, and the initiation or existence of a U.S. Government investigation, that could affect SELLER'S performance under this Contract.

g) SELLER shall be responsible for all losses, costs, claims, causes of action, damages, liabilities and expense, including attorneys' fees, all expense of litigation and/or settlement, and court costs, arising from any act or omission of SELLER, its officers, employees, agents, suppliers, or subcontractors at any tier, in the performance of any of its obligations under this clause that have been finally determined to have been incurred as a direct result of actions or omissions of the SELLER, its officers, employees, agents, suppliers, or subcontractors at any tier.

h) Nothing in these Terms and Conditions add, change, supersede, or waive any of the requirements of applicable Federal laws, Executive Orders, and regulations, including but not limited to –

i. the Export Administration Act of 1979, as amended (50 U.S.C. App. 24 01, et seq.);

ii. the Arms Export Control Act of 1976 (22 U.S.C. 2751, et seq.);

iii. the International Emergency Economic Powers Act (50 U.S.C. 1701, et seq.);

iv. the Export Administration Regulations (15 C.F.R. Parts 730-774);

v. the International Traffic in Arms Regulations (22 C.F.R. Parts 120-130); and

vi. Executive Order 13222, as extended.

i) For the purposes of this Contract, SELLER agrees that this clause shall be inserted in all contractual instruments with subcontractors or suppliers at any tier, and that it will require that its subcontractors and suppliers at any tier to insert it in their contractual instruments, as well.

3. DEFERRED ORDERING OF TECHNICAL DATA OR COMPUTER SOFTWARE

This clause applies to first and second tier subcontractors and vendors:

i. In addition to technical data or computer software that is already subject to a contract delivery requirement, the United States may require at any time the delivery of technical data and non-commercial computer software that has been generated or utilized in the performance of a contract, and compensate the contractor only for reasonable costs incurred for converting and delivering the data in the required form, upon a determination that:

A. the technical data is needed for the purpose or procurement, sustainment, modification, or upgrade (including through competitive means) of a major system or subsystem thereof, a weapon system or subsystem thereof, or any noncommercial item or process; and

I. the technical data –

1. pertains to an item or process developed in whole or in part with Federal funds; or

2. is necessary for the segregation of an item or process from, or the reintegration of that item or process (or a physically or functionally equivalent item or process) with, other items or process, and,

3. Provided that the United States is not foreclosed from requiring the delivery of the technical data by a failure to challenge, in accordance with the requirements of paragraph (e) of the clause entitled “Validation of Restrictive Markings on Technical Data” and paragraph (e) of the clause entitled “Validation of Asserted Restrictions – Computer Software” of this contract, the contractor’s assertion of a use or release restriction on the technical data.

ii. The Government’s rights to use said data or computer software shall be pursuant to the “Rights in Technical Data – Noncommercial Items” and “Rights in Noncommercial Computer Software and Noncommercial Computer Software Documentation” clauses of this contract.

4. LIMITATIONS ON THE USE OR DISCLOSURE OF GOVERNMENT-FURNISHED INFORMATION MARKED WITH RESTRICTIVE LEGENDS

If the Seller will receive Government-furnished information marked with restrictive legends to perform this contract, DFARS 252.227-7025 (JAN 2025) applies to this contract and is incorporated herein by reference.

3052.204-71 Contractor employee access. (with Alt I)

As prescribed in (HSAR) 48 CFR 3004.470-4(a), insert the following clause with appropriate alternates:

Contractor Employee Access (JUL 2023)

(a) *Controlled Unclassified Information (CUI)* is any information the Government creates or possesses, or an entity creates or possesses for or on behalf of the Government (other than classified information) that a law, regulation, or Governmentwide policy requires or permits an agency to handle using safeguarding or dissemination controls. This definition includes the following CUI categories and subcategories of information:

(1) Chemical-terrorism Vulnerability Information (CVI) as defined in 6 CFR part 27, “Chemical Facility Anti-Terrorism Standards,” and as further described in supplementary guidance issued by an authorized official of the Department of Homeland Security (including the Revised Procedural Manual “Safeguarding Information Designated as Chemical-Terrorism Vulnerability Information” dated September 2008);

(2) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (title XXII, subtitle B of the Homeland Security Act of 2002 as amended through Pub. L. 116-283), PCII’s implementing regulations (6 CFR part 29), the PCII Program Procedures Manual, and any supplementary guidance officially communicated by an authorized

official of the Department of Homeland Security, the PCII Program Manager, or a PCII Program Manager Designee;

(3) Sensitive Security Information (SSI) as defined in 49 CFR part 1520, "Protection of Sensitive Security Information," as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or designee), including Department of Homeland Security MD 11056.1, "Sensitive Security Information (SSI)" and, within the Transportation Security Administration, TSA MD 2810.1, "SSI Program";

(4) Homeland Security Agreement Information means information the Department of Homeland Security receives pursuant to an agreement with State, local, Tribal, territorial, or private sector partners that is required to be protected by that agreement. The Department receives this information in furtherance of the missions of the Department, including, but not limited to, support of the Fusion Center Initiative and activities for cyber information sharing consistent with the Cybersecurity Information Sharing Act of 2015;

(5) Homeland Security Enforcement Information means unclassified information of a sensitive nature lawfully created, possessed, or transmitted by the Department of Homeland Security in furtherance of its immigration, customs, and other civil and criminal enforcement missions, the unauthorized disclosure of which could adversely impact the mission of the Department;

(6) International Agreement Information means information the Department of Homeland Security receives that is required to be protected by an information sharing agreement or arrangement with a foreign government, an international organization of governments or any element thereof, an international or foreign public or judicial body, or an international or foreign private or non-governmental organization;

(7) Information Systems Vulnerability Information (ISVI) means:

(i) Department of Homeland Security information technology (IT) systems data revealing infrastructure used for servers, desktops, and networks; applications name, version, and release; switching, router, and gateway information; interconnections and access methods; and mission or business use/need. Examples of ISVI are systems inventories and enterprise architecture models. Information pertaining to national security systems and eligible for classification under Executive Order 13526 will be classified as appropriate; and/or

(ii) Information regarding developing or current technology, the release of which could hinder the objectives of the Department, compromise a technological advantage or countermeasure, cause a denial of service, or provide an adversary with sufficient information to clone, counterfeit, or circumvent a process or system;

(8) Operations Security Information means Department of Homeland Security information that could be collected, analyzed, and exploited by a foreign adversary to identify intentions, capabilities, operations, and vulnerabilities that threaten operational security for the missions of the Department;

(9) Personnel Security Information means information that could result in physical risk to Department of Homeland Security personnel or other individuals whom the Department is responsible for protecting;

(10) Physical Security Information means reviews or reports illustrating or disclosing facility infrastructure or security vulnerabilities related to the protection of Federal buildings, grounds, or property. For example, threat assessments, system security plans, contingency plans, risk management plans, business impact analysis studies, and certification and accreditation documentation;

(11) Privacy Information includes both Personally Identifiable Information (PII) and Sensitive Personally Identifiable Information (SPII). PII refers to information that can be used to distinguish or

trace an individual's identity, either alone, or when combined with other information that is linked or linkable to a specific individual; and SPII is a subset of PII that if lost, compromised, or disclosed without authorization could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. To determine whether information is PII, DHS will perform an assessment of the specific risk that an individual can be identified using the information with other information that is linked or linkable to the individual. In performing this assessment, it is important to recognize that information that is not PII can become PII whenever additional information becomes available, in any medium or from any source, that would make it possible to identify an individual. Certain data elements are particularly sensitive and may alone present an increased risk of harm to the individual.

(i) Examples of stand-alone PII that are particularly sensitive include: Social Security numbers (SSNs), driver's license or State identification numbers, Alien Registration Numbers (A-numbers), financial account numbers, and biometric identifiers.

(ii) Multiple pieces of information may present an increased risk of harm to the individual when combined, posing an increased risk of harm to the individual. SPII may also consist of any grouping of information that contains an individual's name or other unique identifier plus one or more of the following elements:

(A) Truncated SSN (such as last 4 digits);

(B) Date of birth (month, day, and year);

(C) Citizenship or immigration status;

(D) Ethnic or religious affiliation;

(E) Sexual orientation;

(F) Criminal history;

(G) Medical information; and

(H) System authentication information, such as mother's birth name, account passwords, or personal identification numbers (PINs).

(iii) Other PII that may present an increased risk of harm to the individual depending on its context, such as a list of employees and their performance ratings or an unlisted home address or phone number. The context includes the purpose for which the PII was collected, maintained, and used. This assessment is critical because the same information in different contexts can reveal additional information about the impacted individual.

(b) *Information Resources* means information and related resources, such as personnel, equipment, funds, and information technology.

(c) Contractor employees working on this contract must complete such forms as may be necessary for security or other reasons, including the conduct of background investigations to determine suitability. Completed forms shall be submitted as directed by the Contracting Officer. Upon the Contracting Officer's request, the Contractor's employees shall be fingerprinted or subject to other investigations as required. All Contractor employees requiring recurring access to government facilities or access to CUI or information resources are required to have a favorably adjudicated background investigation prior to commencing work on this contract unless this requirement is waived under departmental procedures.

(d) The Contracting Officer may require the Contractor to prohibit individuals from working on the contract if the Government deems their initial or continued employment contrary to the public interest for any reason, including, but not limited to, carelessness, insubordination, incompetence, or security concerns.

(e) Work under this contract may involve access to CUI. The Contractor shall access and use CUI only for the purpose of furnishing advice or assistance directly to the Government in support of the Government's activities, and shall not disclose, orally or in writing, CUI for any other purpose to any

person unless authorized in writing by the Contracting Officer. For those Contractor employees authorized to access CUI, the Contractor shall ensure that these persons receive initial and refresher training concerning the protection and disclosure of CUI. Initial training shall be completed within 60 days of contract award and refresher training shall be completed every 2 years thereafter.

(f) The Contractor shall include this clause in all subcontracts at any tier where the subcontractor may have access to government facilities, CUI, or information resources.

(g) Before receiving access to information resources under this contract, the individual must complete a security briefing; additional training for specific categories of CUI, if identified in the contract; and any nondisclosure agreement furnished by DHS. The Contracting Officer's Representative (COR) will arrange the security briefing and any additional training required for specific categories of CUI.

(h) The Contractor shall have access only to those areas of DHS information resources explicitly stated in this contract or approved by the COR in writing as necessary for performance of the work under this contract. Any attempts by Contractor personnel to gain access to any information resources not expressly authorized by the terms and conditions in this contract, or as approved in writing by the COR, are strictly prohibited. In the event of violation of this provision, DHS will take appropriate actions with regard to the contract and the individual(s) involved.

(i) Contractor access to DHS networks from a remote location is a temporary privilege for mutual convenience while the Contractor performs business for DHS. It is not a right, a guarantee of access, a condition of the contract, or government-furnished equipment (GFE).

(j) Contractor access will be terminated for unauthorized use. The Contractor agrees to hold and save DHS harmless from any unauthorized use and agrees not to request additional time or money under the contract for any delays resulting from unauthorized use or access.

(k) Non-U.S. citizens shall not be authorized to access or assist in the development, operation, management, or maintenance of Department IT systems under the contract, unless a waiver has been granted by the Head of the Component or designee, with the concurrence of both the Department's Chief Security Officer (CSO) and the Chief Information Officer (CIO) or their designees. Within DHS Headquarters, the waiver may be granted only with the approval of both the CSO and the CIO or their designees. In order for a waiver to be granted:

(1) There must be a compelling reason for using this individual as opposed to a U.S. citizen; and

(2) The waiver must be in the best interest of the Government.

(l) Contractors shall identify in their proposals the names and citizenship of all non-U.S. citizens proposed to work under the contract. Any additions or deletions of non-U.S. citizens after contract award shall also be reported to the Contracting Officer.