FAIRBANKS MORSE LLC
SUPPLEMENTAL PURCHASING TERMS AND CONDITIONS
FLOWDOWN CLAUSES FOR PURCHASE ORDERS ISSUED IN SUPPORT OF THE 270' MEDIUM ENDURANCE CUTTER SERVICE LIFE EXTENSION PROGRAM

1. INCORPORATION BY REFERENCE. These Supplemental Purchasing Terms and Conditions are incorporated in their entirety into any Purchase Order issued in support of the 270' Medium Endurance Cutter Service Life Extension Program. In the event of a conflict between these Supplemental Purchasing Terms and Conditions and the Fairbanks Morse Terms and Conditions of Purchase, these Supplemental Purchasing Terms and Conditions shall prevail.

2. CERTIFICATIONS. By accepting or performing this Purchase Order, Seller certifies that:

a. Neither Seller nor any of its Principals are presently debarred, suspended, proposed for debarment, or declared ineligible for the award of contracts by any Federal agency. "Principal" means an officer, director, owner, partner, or a person having primary management or supervisory responsibilities within a business entity (*e.g.*, general manager; plant manager; head of a division or business segment; and similar positions).

b. Neither Seller nor any of its affiliates are owned or controlled by the government of a country that is a state sponsor of terrorism.

c. Seller: (i) is in compliance with Sec. 202 of Executive Order 11246, as amended by Executive Order 11375, and subsequent Executive Orders and the Rules and Regulations set forth by the Secretary of Labor in effect as of the date of this Executive Order; (ii) does not and will not provide or maintain at any of its establishments, nor permit its employees to perform their services at any location under its control where there are maintained segregated facilities; and (iii) agrees that a breach of this Certification violates the Equal Employment clause of Executive Order 11246. "Segregated Facilities" means facilities which are in fact segregated on a basis of race, color, religion, sex, sexual orientation, gender identity, or national origin. Seller agrees to: (1) obtain an identical certification from proposed subcontractors prior to the award of subcontracts exceeding $10,000 which are not exempt from the provisions of the Equal Opportunity clause; and (2) maintain such certifications in its files. The penalty for making a false representation is prescribed under 18 U.S.C. 1001 and any such false representation shall be a material breach of this Purchase Order.

d. If it has participated in a previous prime contract or subcontract subject to FAR 52.222-26, "Equal Opportunity," that Seller has filed all required compliance reports.

e. If it has previously had contracts subject to the written affirmative action programs requirement of the rules and regulations of the Secretary of Labor (41 CFR 60-1 and 60-2), that Seller has developed and has on file at each establishment affirmative action programs required by such rules and regulations.

f. If Seller is registered in the System for Award Management ("SAM"), the size or socioeconomic representations and certifications in SAM (or any other successor system) are current, accurate and complete as of the date of Seller's offer.

g. To the best of its knowledge and belief that no Federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, or an employee of a Member of Congress on its behalf in connection with the awarding of this Purchase Order. If any registrants under the Lobbying Disclosure Act of 1995 have made a lobbying contact on behalf of Seller with respect to this Purchase Order, Seller shall complete and submit, with its offer, OMB Standard Form LLL, Disclosure of Lobbying Activities, to provide the name of the registrants. Seller need not report regularly employed officers or employees of Seller to whom payments of reasonable compensation were made. Submission of this certification and disclosure is a prerequisite for making or entering into this Purchase Order imposed by 31 U.S.C. 1352. Any person who makes an expenditure prohibited under this provision or who fails to file or amend the disclosure required to be filed or amended by this provision, shall be subject to a civil penalty of not less than $10,000, and not more than $100,000, for each such failure. As used in this Certification, "Lobbying contact" has the meaning provided at 2 U.S.C. 1602(8) and the remaining terms are defined in FAR clause 52.203-12, "Limitation on Payments to Influence Certain Federal Transactions."

h. Seller will not provide "covered telecommunications equipment or services," as defined in FAR 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment, to Buyer in the performance of this or any Purchase Order.

3. EQUAL EMPLOYMENT OPPORTUNITY. Buyer and Seller shall abide by the requirements of 41 CFR §§ 60-1.4(a), 60-300.5(a), 60-741.5(a) and 29 CFR Part 471, Appendix A to Subpart A. These regulations prohibit discrimination against qualified individuals based on their status as protected veterans or individuals with disabilities, and prohibit discrimination against all individuals based on their race, color, religion, sex, sexual orientation, gender identity or expression, or national origin. Moreover, these regulations require that covered prime contractors and subcontractors take affirmative action to employ and advance in employment individuals without regard to race, color, religion, sex, sexual orientation, gender identity or expression, national origin, protected veteran status or disability. Seller shall include this Paragraph 3 in each lower-tier subcontract it issues.

4. EXPORT CONTROLS AND ECONOMIC SANCTIONS.

a. Seller agrees to comply with all applicable export control and economic sanctions laws including, but not limited to: (i) the Export Administration Regulations ("EAR") administered by the U.S. Department of Commerce; (ii) the International Traffic in Arms Regulations ("ITAR") administered by the U.S. Department of State; (iii) the various economic sanctions programs administered by the U.S. Department of Treasury's Office of Foreign Assets Control ("OFAC regulations") and the U.S. Department of State's Office of Terrorism Finance and Economic Sanctions Policy; and (iv) any and all export controls or economic sanctions maintained by the European Union ("EU"), United

Kingdom or any other governmental authority to which Seller is subject (collectively "Export Control Laws").

b. Seller shall obtain and maintain any and all authorizations, licenses and registrations required under the aforementioned Export Control Laws, including those required for the sale under this Purchase Order to Buyer. Seller will furnish Buyer with: (i) documentation identifying any articles, services, software, technology and/or technical data subject to these Export Control Laws; (ii) written confirmation of the relevant Export Classification Control Numbers ("ECCNs"), U.S. Munition List ("USML") category numbers or other export classification designators for each such item; and (iii) copies of any related export licenses or authorizations. If Seller sources such items outside the United States, then Seller shall notify Buyer and take all necessary measures to comply with all foreign Export Control Laws that may relate to the sale or transfer of the same.

c. Seller shall clearly and appropriately label any controlled technical data (including, but not limited to, drawings, designs, specifications, blueprints, computer-aided design (CAD) information and other technical documents or electronic information related to the production, manufacture or maintenance of a controlled article) that it provides to Buyer as controlled pursuant to the EAR, ITAR and/or other applicable laws. Seller shall provide any controlled technical data communicated to Buyer using secure communication protocols designed for the purpose of complying with the Export Control Laws. Under no circumstances should such information be emailed using systems that are not designed for the secure communication of controlled technical data.

d. Seller agrees that it will not source any articles, services, software, technology or technical data that originate from any country, government, organization or person that is: (i) subject to U.S., EU or British economic sanctions or other applicable sanction regimes; or (ii) debarred or restricted pursuant to the aforementioned Export Control Laws, or the U.S. Department of Defense Federal Acquisition Regulation Supplement.

e. Seller is solely and exclusively responsible for safeguarding all export controlled articles, services, software, technology or technical data until Buyer receives the items at issue. This includes both exports to a non-U.S. destination and allowing non-U.S. persons to access such items while located within the United States. Seller will also take appropriate steps to ensure that no export controlled articles, services, software, technology or technical data can be shipped to a controlled country (or otherwise accessed by unauthorized foreign nationals) without the appropriate export licenses. Where Seller is shipping a controlled article, Seller shall use a carrier that maintains procedures designed to comply with the Export Control Laws, and provide any required notifications to the carrier that the shipment involves controlled items.

f. If Seller is a signatory to a Technical Assistance Agreement ("TAA") or Manufacturing License Agreement ("MLA") with Buyer, Seller shall promptly notify Buyer of any changed circumstances that would require modifying the terms of such an agreement, including any potential violation of the terms of the agreement, any ineligibility to export, any investigation into alleged violations of any of the Export Control Laws, any self-disclosure of potential export controls violations, any addition of foreign personnel to

any project covered by such an agreement or any other circumstances that may affect Seller's ability to perform pursuant to the terms of the agreement.

g. Seller shall immediately notify Buyer if it is or becomes listed on any Excluded or Denied Party List maintained by any U.S., EU or British agency, or if any government denies, suspends or revokes its export privileges.

h. Seller shall prepare and provide accurate invoices and documentation for each shipment that will allow Buyer to comply with the export and import requirements administered by U.S. Customs & Border Protection ("CBP"). Such invoices and/or documentation shall include: (i) Seller's name and address; (ii) the terms of sale; (iii) the total quantity of goods being shipped; (iv) a description of the goods being shipped; (v) the country of origin of the goods; (vi) the valuation of the goods; (vii) the currency in which the goods are priced; and (viii) any discounts that have been included for the shipment that are not otherwise reflected in the unit price.

i. Seller shall promptly notify Buyer in writing of any suspected violation of the aforementioned Export Control Laws of which it becomes aware. Seller further agrees that it will fully cooperate in any investigation by or on behalf of Buyer related to the subject matter of the Purchase Order, including by providing full access to relevant personnel and records to aid Buyer in the identification and evaluation of any suspected violation, following reasonable notice from Buyer.

j. Seller shall indemnify, defend and hold harmless Buyer and Buyer's parent companies, subsidiaries, affiliates, shareholders, members, partners, directors, managers, officers, employees, insurers, agents, customers, successors and assigns from and against any and all claims, demands, actions, losses, injuries, damages, liabilities, obligations, penalties, costs and expenses, including attorneys' fees, experts' fees and other costs of defending any claim, demand or action (including costs of investigation of potential violations of the Export Control Laws) (collectively, "Losses") that may arise as a result of Seller's breach of any of the provisions within this Paragraph 4.

5. COMPTROLLER GENERAL EXAMINATION OF RECORD. The Comptroller General of the United States, an appropriate Inspector General appointed under section 3 or 8G of the Inspector General Act of 1978 (5 U.S.C. App.), or an authorized representative of either of the foregoing officials shall have access to and right to examine any of Seller's or any subcontractors' records that pertain to, and involve transactions relating to, this Purchase Order. Seller shall make available at its offices at all reasonable times the records, materials, and other evidence for examination, audit, or reproduction, until 3 years after final payment under this Purchase Order or for any shorter period specified in FAR Subpart 4.7, Contractor Records Retention, of the other clauses of this Purchase Order. If this Purchase Order is completely or partially terminated, the records relating to the work terminated shall be made available for 3 years after any resulting final termination settlement. Records relating to appeals or to litigation or the settlement of claims arising under or relating to this Purchase Order shall be made available until such appeals, litigation, or claims are finally resolved. As used in this Paragraph 5, records include books, documents, accounting procedures and practices, and other data, regardless of type and regardless of form. This does not require Seller to create or maintain

any record that Seller does not maintain in the ordinary course of business or pursuant to a provision of law.

6. DISPUTES.

a. If Buyer elects to prosecute any dispute involving this Purchase Order under the disputes procedure applicable to the U.S. Government prime contract, Seller shall cooperate fully with Buyer in prosecuting the dispute. Seller shall be bound by the final outcome of the disputes procedure if: (i) Buyer has afforded Seller an opportunity to participate in Buyer's prosecution of the dispute; or (ii) Buyer, having decided to discontinue its own prosecution of the dispute, has afforded Seller an opportunity to continue to prosecute the dispute in Buyer's name. Buyer and Seller shall each bear their own costs of prosecuting any dispute.

b. Pending the final resolution of any dispute arising out of or relating to this Purchase Order, Seller shall proceed diligently with performance of this Purchase Order, including the delivery of goods and performance of services, in accordance with Buyer's direction.

7. CHANGES.

a. For any changes issued in accordance with Paragraph 22 of Buyer's Terms and Conditions of Purchase, Seller must assert its right to an adjustment within fifteen (15) days from the date of receipt of the written order. However, if Buyer decides that the facts justify it, Buyer may receive and act upon a proposal submitted before final payment of this Purchase Order. Buyer has the right to examine any of Seller's pertinent books and records for the purpose of verifying Seller's claim.

b. Seller shall immediately proceed with the performance of this Purchase Order as changed. Failure to agree to any adjustment shall be a dispute within the meaning of the "Disputes" provision above. Seller shall not be entitled to any claim for changes unless authorized in writing by Buyer.

8. LIMITATION OF LIABILITY.

a. In no event shall Buyer be liable to Seller (i) for any punitive, exemplary or other special damages arising under or relating to this Purchase Order or the subject matter hereof (ii) for any indirect, incidental or consequential damages (including, without limitation, loss of use, income, profits or anticipated profits, business or business opportunity, savings, data, or business reputation) arising under or relating to this Purchase Order or the subject matter hereof, regardless of whether such damages are based in contract, breach of warranty, tort, negligence or any other theory, and regardless of whether Buyer has been advised of, knew of, or should have known of the possibility of such damages.

b. The maximum aggregate liability of Buyer to Seller arising out of or relating to this Purchase Order shall not exceed the purchase price for the goods or services at issue in the claim.

9. EXCUSABLE DELAYS. Seller shall be liable for default unless nonperformance is caused by an occurrence beyond the reasonable control of Seller and without its fault or negligence, such as acts of God or the public enemy, acts of the Government in either its sovereign or contractual capacity, fires, floods, epidemics, quarantine restrictions, strikes, unusually severe weather, and delays of common carriers. Seller shall notify Buyer in writing as soon as it is reasonably possible after the commencement of any excusable delay, setting forth the full particulars in connection therewith, shall remedy such occurrence with all reasonable dispatch, and shall promptly give written notice to Buyer of the cessation of such occurrence. This Purchase Order is subject to modification or cancellation by Buyer in the event of fire, act of God, public enemy, earthquake, floods, strikes, labor troubles, pandemics or any other cause beyond Buyer's reasonable control.

10. TERMINATION FOR CONVENIENCE. Buyer reserves the right to terminate this Purchase Order, or any part hereof, for its sole convenience. In the event of such termination, Seller shall immediately stop all work hereunder and shall immediately cause any and all of its suppliers and subcontractors to cease work. Subject to the terms of this Purchase Order, Seller shall be paid a percentage of the Purchase Order price reflecting the percentage of the work performed prior to the notice of termination, plus reasonable charges Seller can demonstrate to the satisfaction of Buyer using its standard record keeping system, have resulted from the termination. Seller shall not be required to comply with the cost accounting standards or contract cost principles for this purpose. Seller shall not be paid for any work performed or costs incurred which reasonably could have been avoided.

11. TERMINATION FOR CAUSE. Buyer may terminate this Purchase Order, or any part hereof, for cause in the event of any default by Seller, or if Seller fails to comply with any Purchase Order terms and conditions, or fails to provide Buyer, upon request, with adequate assurances of future performance. In the event of termination for cause, Buyer shall not be liable to Seller for any amount for supplies or services not accepted, and Seller shall be liable to Buyer for any and all rights and remedies provided by law. If it is determined that Buyer improperly terminated this Purchase Order for default, such termination shall be deemed a termination for convenience.

12. FAR/HSAR CLAUSES.

a. The following clauses set forth in the Federal Acquisition Regulation ("FAR" available at http://www.acquisition.gov/FAR) and the Homeland Security Acquisition Regulation ("HSAR" available at https://www.acquisition.gov/hsar) in effect as of the date identified below are incorporated herein by reference with the same force and effect as if they were given in full text. For purposes of this Purchase Order, the following clauses shall operate, impose the obligations and responsibilities of the parties and be interpreted as if "Government" means "Buyer," "Contracting Officer" means an authorized representative of Buyer's purchasing department, "Contract" means this "Purchase Order," "Offeror" means "Seller," "Contractor" means "Seller," and "Disputes

clause" means the Disputes clause of this Purchase Order. Seller shall also include these FAR and HSAR clauses in each lower-tier subcontract it issues, as applicable.

b. "COTS item" means any item of supply (including construction material) that is: (i) a commercial item (as defined in paragraph (1) of the commercial item definition FAR 2.101); (ii) sold in substantial quantities in the commercial marketplace; and (iii) offered to Buyer under this Purchase Order without modification, in the same form in which it is sold in the commercial marketplace.

c. "Prime Contract" means the contract with the U.S. Government under which this Purchase Order is issued.

FAR	**Clauses**	**Date**
52.202-1	Definitions	NOV 2013
52.203-3	Gratuities	APR 1984
52.203-5	Covenant Against Contingent Fees	MAY 2014
52.203-6	Restrictions on Subcontractor Sales to the Government (applies to Purchase Orders with a value over $250,000)	SEP 2006
52.203-7	Anti-Kickback Procedures (except paragraph (c)(1), applies to Purchase Orders with a value over $150,000)	MAY 2014
52.203-8	Cancellation, Rescission, and Recovery of Funds for Illegal or Improper Activity	MAY 2014
52.203-10	Price or Fee Adjustment for Illegal or Improper Activity	MAY 2014
52.203-12	Limitation on Payments to Influence Certain Federal Transactions (applies to Purchase Orders with a value over $150,000)	OCT 2010
52.203-13	Contractor Code of Business Ethics and Conduct (applies to Purchase Orders that have a: (i) value exceeding $5.5 million; and (ii) performance period of more than 120 days; all disclosures of violation of the civil False Claims Act or of Federal criminal law shall be directed to the agency Officer of the Inspector General, with a copy to the Contracting Officer for the Prime Contract)	OCT 2015
52.203-15	Whistleblower Protections under the American Recovery and Reinvestment Act of (2009) (applies to Purchase Orders funded in whole or in part with Recovery Act funds)	JUN 2010
52.203-19	Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements	JAN 2017
52.204-9	Personal Identity Verification of Contractor Personnel (applies to Purchase Orders when Seller's employees are required to have routine physical access to a Federally-controlled facility or routine access to a Federally-controlled information system; Seller shall return to Buyer the identification issued under the clause)	JAN 2011

52.204-23	Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities	JUL 2018
52.204-25	Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment	AUG 2019
52.209-6	Protecting the Government's Interest When Subcontracting with Contractors Debarred, Suspended, or Proposed for Debarment (applies to Purchase Orders with a value over $35,000, other than Purchase Orders for COTS items)	OCT 2015
52.209-10	Prohibition on Contracting with Inverted Domestic Corporations	NOV 2015
52.219-8	Utilization of Small Business Concerns	OCT 2018
52.219-28	Post Award Small Business Rerepresentation	MAR 2020
52.222-3	Convict Labor	JUN 2003
52.222-19	Child Labor – Cooperation with Authorities and Remedies	JAN 2020
52.222-21	Prohibition of Segregated Facilities	APR 2015
52.222-26	Equal Opportunity	SEP 2016
52.222-35	Equal Opportunity for Veterans (applies to Purchase Orders with a value of $150,000 or more)	OCT 2015
52.222-36	Equal Opportunity for Workers with Disabilities (applies to Purchase Orders with a value in excess of $15,000)	JUL 2014
52.222-37	Employment Reports on Veterans (applies to Purchase Orders with a value of $150,000 or more)	FEB 2016
52.222-40	Notification of Employee Rights Under the National Labor Relations Act (applies to Purchase Orders that exceed $10,000 and will be wholly or partially performed in the United States)	DEC 2010
52.222-41	Service Contract Labor Standards (applies to Purchase Orders for the performance of services subject to the Service Contract Labor Standards statute)	AUG 2018
52.222-42	Statement of Equivalent Rates for Federal Hires (applies to Purchase Orders for the performance of services subject to the Service Contract Labor Standards statute)	MAY 2014
52.222-44	Fair Labor Standards Act and Service Contract Labor Standards – Price Adjustment (applies to Purchase Orders for the performance of services subject to the Service Contract Labor Standards statute)	MAY 2014
52.222-50	Combating Trafficking in Persons	JAN 2019
52.222-54	Employment Eligibility Verification (applies to Purchase Orders for the performance of services that includes work performed in the United States and has a value over $3,500; not applicable if the Purchase Order is for commercial services that are part of the purchase of a COTS item (or an	OCT 2015

	item that would be a COTS item, but for minor modifications) performed by the COTS provider)	
52.222-55	Minimum Wages Under Executive Order 13658 (applies to Purchase Orders (applies to Purchase Orders for the performance of services subject to the Service Contract Labor Standards statute)	DEC 2015
52.222-62	Paid Sick Leave Under Executive Order 13706 (applies to Purchase Orders for the performance of services subject to the Service Contract Labor Standards statute)	JAN 2017
52.223-3	Hazardous Material Identification and Material Safety Data	JAN 1997
52.223-10	Waste Reduction Program	MAY 2011
52.223-19	Compliance with Environmental Management Systems	MAY 2011
52.224-3	Privacy Training (applicable if Seller's employees will perform the work specified in paragraph (f) of the clause)	JAN 2017
52.225-13	Restrictions on Certain Foreign Purchases	JUN 2008
52.225-26	Contractors Performing Private Security Functions Outside the United States (applies to Purchase Orders that will be performed outside the U.S. in areas of combat operations, as designated by the Secretary of Defense, or other significant military operations, upon agreement of the Secretaries of Defense and State that the clause applies in that area)	OCT 2016
52.227-14	Rights in Data – General (References to the "Government" shall mean the U.S. Government and references to the "Contracting Officer" shall mean the U.S. Government Contracting Officer for the Prime Contract)	MAY 2014
52.232-39	Unenforceability of Unauthorized Obligations	JUN 2013
52.232-40	Providing Accelerated Payments to Small Business Subcontractors (applies to Purchase Orders with small business concerns)	DEC 2013
52.233-3	Protest After Award (in paragraph (b)(2), the term "30 days" is changed to "15 days")	AUG 1996
52.237-2	Protection of Government Buildings, Equipment, and Vegetation	APR 1982
52.242-13	Bankruptcy	JUL 1995
52.247-21	Contractor Liability for Personal Injury and/or Property Damage (applies to Purchase Orders for transportation or transportation related services)	APR 1984
52.247-64	Preference for Privately Owned U.S.-Flag Commercial Vessels	FEB 2006
HSAR	**Clauses**	**Date**
3052.203-70	Instructions for Contractor Disclosure of Violations (references herein to "Contracting Officer" shall remain the Contracting Officer for the Prime Contract)	SEP 2012

3052.204-71	Contractor Employee Access (applies if Seller may have access to Government facilities, sensitive information, or resources)	SEP 2012
3052.205-70	Advertisement, Publicizing Awards, and Releases (references herein to the "Federal Government" or "Government" shall mean the Federal Government or Buyer).	SEP 2012
3052.222-70	Strikes or Picketing Affecting Timely Completion of the Contract Work	DEC 2003
3052.223-90	Accident and Fire Reporting	DEC 2003

FAR 52.203-17 CONTRACTOR EMPLOYEE WHISTLEBLOWER RIGHTS AND REQUIREMENT TO INFORM EMPLOYEES OF WHISTLEBLOWER RIGHTS (APR 2014) (DHS-USCG DEVIATION 14-01)

(a) This contract and employees working on this contract will be subject to the whistleblower rights and remedies in the pilot program on Contractor employee whistleblower protections established at 41 U.S.C. 4712 by section 828 of the National Defense Authorization Act for Fiscal Year 2013 (Pub. L. 112-239) and FAR 3.908.

(b) The Contractor shall inform its employees in writing, in the predominant language of the workforce, of employee whistleblower rights and protections under 41 U.S.C. 4712, as described in section 3.908 of the Federal Acquisition Regulation.

(c) The Contractor shall insert the substance of this clause, including this paragraph (c), in all subcontracts over the simplified acquisition threshold ($150,000).

(End of clause)

13. OTHER PRIME CONTRACT CLAUSES. The following clause contained in Buyer's Prime Contract, is incorporated into this Purchase Order as set forth below (modified as necessary to properly identify the parties to this Purchase Order),:

HSAR Class Deviation 15-01 SAFEGUARDING OF SENSITIVE INFORMATION (MAR 2015)

(a) *Applicability.* This clause applies to Seller, its subcontractors, and Seller employees (hereafter referred to collectively as "Seller"). Seller shall insert the substance of this clause in all subcontracts.

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

"Personally Identifiable Information (PII)" means information that can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, either alone, or when combined with other personal or identifying information that is linked or linkable

to a specific individual, such as date and place of birth, or mother's maiden name. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-personally identifiable information can become personally identifiable information whenever additional information is made publicly available—in any medium and from any source—that, combined with other available information, could be used to identify an individual.

PII is a subset of sensitive information. Examples of PII include, but are not limited to: name, date of birth, mailing address, telephone number, Social Security number (SSN), email address, zip code, account numbers, certificate/license numbers, vehicle identifiers including license plates, uniform resource locators (URLs), static Internet protocol addresses, biometric identifiers such as fingerprint, voiceprint, iris scan, photographic facial images, or any other unique identifying number or characteristic, and any information where it is reasonably foreseeable that the information will be linked with other information to identify the individual.

"Sensitive Information" is defined in HSAR clause 3052.204-71, Contractor Employee Access, as any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of Title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

(1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);

(2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, "Policies and Procedures of Safeguarding and Control of SSI," 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 his/her designee);

(3) Information designated as "For Official Use Only," which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and

(4) Any information that is designated "sensitive" or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.

"Sensitive Information Incident" is an incident that includes the known, potential, or suspected or unauthorized access or attempted access of any Government system, contractor system, or sensitive information.

"Sensitive Personally Identifiable Information (SPII)" is a subset of PII, which if lost, compromised or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some forms of PII are sensitive as stand-alone elements. Examples of such PII include: Social Security numbers (SSN), driver's license or state identification number, Alien Registration Numbers (A-number), financial account number, and biometric identifiers such as fingerprint, voiceprint, or iris scan. Additional examples include any groupings of information that contain an individual's name or other unique identifier plus one or more of the following elements:

(1) Truncated SSN (such as last 4 digits)
(2) Date of birth (month, day, and year)
(3) Citizenship or immigration status
(4) Ethnic or religious affiliation
(5) Sexual orientation
(6) Criminal History
(7) Medical Information
(8) System authentication information such as mother's maiden name, account passwords or personal identification numbers (PIN)

Other PII may be "sensitive" depending on its context, such as a list of employees and their performance ratings or an unlisted home address or phone number. In contrast, a business card or public telephone directory of agency employees contains PII but is not sensitive.

(c) *Authorities.* Seller shall follow all current versions of Government policies and guidance accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors, or available upon request from the Contracting Officer, including but not limited to:

(1) DHS Management Directive 11042.1 Safeguarding Sensitive But Unclassified (for Official Use Only) Information
(2) DHS Sensitive Systems Policy Directive 4300A
(3) DHS 4300A Sensitive Systems Handbook and Attachments
(4) DHS Security Authorization Process Guide
(5) DHS Handbook for Safeguarding Sensitive Personally Identifiable Information
(6) DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program
(7) DHS Information Security Performance Plan (current fiscal year)
(8) DHS Privacy Incident Handling Guidance
(9) Federal Information Processing Standard (FIPS) 140-2 Security Requirements for Cryptographic Modules accessible at http://csrc.nist.gov/groups/STM/cmvp/standards.html
(10) National Institute of Standards and Technology (NIST) Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations accessible at http://csrc.nist.gov/publications/PubsSPs.html

(11) NIST Special Publication 800-88 Guidelines for Media Sanitization accessible at http://csrc.nist.gov/publications/PubsSPs.html

(d) *Handling of Sensitive Information.* Seller compliance with this clause, as well as the policies and procedures described below, is required.

(1) Department of Homeland Security (DHS) policies and procedures on contractor personnel security requirements are set forth in various Management Directives (MDs), Directives, and Instructions. *MD 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information* describes how contractors must handle sensitive but unclassified information. DHS uses the term "FOR OFFICIAL USE ONLY" to identify sensitive but unclassified information that is not otherwise categorized by statute or regulation. Examples of sensitive information that are categorized by statute or regulation are PCII, SSI, etc. The *DHS Sensitive Systems Policy Directive 4300A* and the *DHS 4300A Sensitive Systems Handbook* provide the policies and procedures on security for Information Technology (IT) resources. The *DHS Handbook for Safeguarding Sensitive Personally Identifiable Information* provides guidelines to help safeguard SPII in both paper and electronic form. *DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program* establishes procedures, program responsibilities, minimum standards, and reporting protocols for the DHS Personnel Suitability and Security Program.

(2) Seller shall not use or redistribute any sensitive information processed, stored, and/or transmitted by Seller except as specified in the contract.

(3) All Seller employees with access to sensitive information shall execute *DHS Form 11000-6, Department of Homeland Security Non-Disclosure Agreement (NDA),* as a condition of access to such information. Seller shall maintain signed copies of the NDA for all employees as a record of compliance. Seller shall provide copies of the signed NDA to Buyer no later than two (2) days after execution of the form.

(4) Seller's invoicing, billing, and other recordkeeping systems maintained to support financial or other administrative functions shall not maintain SPII. It is acceptable to maintain in these systems the names, titles and contact information for the COR or other Government personnel associated with the administration of the contract, as needed.

(e) *Authority to Operate*. Seller shall not input, store, process, output, and/or transmit sensitive information within a Seller IT system without an Authority to Operate (ATO) signed by the Headquarters or Component CIO, or designee, in consultation with the Headquarters or Component Privacy Officer. Unless otherwise specified in the ATO letter, the ATO is valid for three (3) years. Seller shall adhere to current Government policies, procedures, and guidance for the Security Authorization (SA) process as defined below.

(1) Complete the Security Authorization process. The SA process shall proceed according to the *DHS Sensitive Systems Policy Directive 4300A* (Version 11.0, April 30, 2014), or any successor publication, *DHS 4300A Sensitive Systems Handbook* (Version 9.1, July 24, 2012), or any successor publication, and the *Security Authorization Process Guide* including templates.

(i) Security Authorization Process Documentation. SA documentation shall be developed using the Government provided Requirements Traceability Matrix and Government security documentation templates. SA documentation consists of the following: Security Plan, Contingency Plan, Contingency Plan Test Results, Configuration Management Plan, Security Assessment Plan, Security Assessment Report, and Authorization to Operate Letter. Additional documents that may be required include a Plan(s) of Action and Milestones and Interconnection Security Agreement(s). During the development of SA documentation, Seller shall submit a signed SA package, validated by an independent third party, to the COR for acceptance by the Headquarters or Component CIO, or designee, at least thirty (30) days prior to the date of operation of the IT system. The Government is the final authority on the compliance of the SA package and may limit the number of resubmissions of a modified SA package. Once the ATO has been accepted by the Headquarters or Component CIO, or designee, the Contracting Officer shall incorporate the ATO into the contract as a compliance document. The Government's acceptance of the ATO does not alleviate Seller's responsibility to ensure the IT system controls are implemented and operating effectively.

(ii) Independent Assessment. Seller shall have an independent third party validate the security and privacy controls in place for the system(s). The independent third party shall review and analyze the SA package, and report on technical, operational, and management level deficiencies as outlined in *NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations*. Seller shall address all deficiencies before submitting the SA package to the Government for acceptance.

(iii) Support the completion of the Privacy Threshold Analysis (PTA) as needed. As part of the SA process, Seller may be required to support the Government in the completion of the PTA. The requirement to complete a PTA is triggered by the creation, use, modification, upgrade, or disposition of a Seller IT system that will store, maintain and use PII, and must be renewed at least every three (3) years. Upon review of the PTA, the DHS Privacy Office determines whether a Privacy Impact Assessment (PIA) and/or Privacy Act System of Records Notice (SORN), or modifications thereto, are required. Seller shall provide all support necessary to assist the Department in completing the PIA in a timely manner and shall ensure that project management plans and schedules include time for the completion of the PTA, PIA, and SORN (to the extent required) as milestones. Support in this context includes responding timely to requests for information from the Government about the use, access, storage, and maintenance of PII on Seller's system, and providing timely review of relevant compliance documents for factual accuracy. Information on the DHS privacy compliance process, including PTAs, PIAs, and SORNs, is accessible at http://www.dhs.gov/privacy-compliance.

(2) *Renewal of ATO*. Unless otherwise specified in the ATO letter, the ATO shall be renewed every three (3) years. Seller is required to update its SA package as part of the ATO renewal process. Seller shall update its SA package by one of the following methods:

(1) Updating the SA documentation in the DHS automated information assurance tool for acceptance by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls; or

(2) Submitting an updated SA package directly to the COR for approval by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls. The 90 day review process is independent of the system production date and therefore it is important that Seller build the review into project schedules. The reviews may include onsite visits that involve physical or logical inspection of Seller environment to ensure controls are in place.

(3) *Security Review.* The Government may elect to conduct random periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. Seller shall afford DHS, the Office of the Inspector General, and other Government organizations access to Seller's facilities, installations, operations, documentation, databases and personnel used in the performance of this contract. Seller shall, through the Contracting Officer and COR, contact the Headquarters or Component CIO, or designee, to coordinate and participate in review and inspection activity by Government organizations external to the DHS. Access shall be provided, to the extent necessary as determined by the Government, for the Government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability and confidentiality of Government data or the function of computer systems used in performance of this contract and to preserve evidence of computer crime.

(4) *Continuous Monitoring.* All Seller-operated systems that input, store, process, output, and/or transmit sensitive information shall meet or exceed the continuous monitoring requirements identified in the *Fiscal Year 2014 DHS Information Security Performance Plan*, or successor publication. The plan is updated on an annual basis. Seller shall also store monthly continuous monitoring data at its location for a period not less than one year from the date the data is created. The data shall be encrypted in accordance with *FIPS 140-2 Security Requirements for Cryptographic Modules* and shall not be stored on systems that are shared with other commercial or Government entities. The Government may elect to perform continuous monitoring and IT security scanning of Seller systems from Government tools and infrastructure.

(5) *Revocation of ATO.* In the event of a sensitive information incident, the Government may suspend or revoke an existing ATO (either in part or in whole). If an ATO is suspended or revoked in accordance with this provision, the Contracting Officer may direct Seller to take additional security measures to secure sensitive information. These measures may include restricting access to sensitive information on Seller IT system under this contract. Restricting access may include disconnecting the system processing, storing, or transmitting the sensitive information from the Internet or other networks or applying additional security controls.

(6) *Federal Reporting Requirements.* Sellers operating information systems on behalf of the Government or operating systems containing sensitive information shall comply with Federal reporting requirements. Annual and quarterly data collection will be coordinated by the Government. Seller shall provide the COR with requested information within three (3) business days of receipt of the request. Reporting requirements are determined by the Government and are defined in the *Fiscal Year 2014 DHS Information Security Performance Plan*, or successor publication. Seller shall provide the Government with all information to fully satisfy Federal reporting requirements for Seller systems.

(f) *Sensitive Information Incident Reporting Requirements.*

(1) All known or suspected sensitive information incidents shall be reported to the Headquarters or Component Security Operations Center (SOC) within one hour of discovery in accordance with *4300A Sensitive Systems Handbook Incident Response and Reporting* requirements. When notifying the Headquarters or Component SOC, Seller shall also notify the Contracting Officer, COR, Headquarters or Component Privacy Officer, and US-CERT using the contact information identified in the contract. If the incident is reported by phone or the Contracting Officer's email address is not immediately available, Seller shall contact the Contracting Officer immediately after reporting the incident to the Headquarters or Component SOC. Seller shall not include any sensitive information in the subject or body of any e-mail. To transmit sensitive information, Seller shall use *FIPS 140-2 Security Requirements for Cryptographic Modules* compliant encryption methods to protect sensitive information in attachments to email. Passwords shall not be communicated in the same email as the attachment. A sensitive information incident shall not, by itself, be interpreted as evidence that Seller has failed to provide adequate information security safeguards for sensitive information, or has otherwise failed to meet the requirements of the contract.

(2) If a sensitive information incident involves PII or SPII, in addition to the reporting requirements in *4300A Sensitive Systems Handbook Incident Response and Reporting*, Seller shall also provide as many of the following data elements that are available at the time the incident is reported, with any remaining data elements provided within 24 hours of submission of the initial incident report:

(i) Data Universal Numbering System (DUNS);
(ii) Contract numbers affected unless all contracts by the company are affected;
(iii) Facility CAGE code if the location of the event is different than the prime contractor location; (iv) Point of contact (POC) if different than the POC recorded in the System for Award Management (address, position, telephone, email);
(v) Contracting Officer POC (address, telephone, email);
(vi) Contract clearance level;
(vii) Name of subcontractor and CAGE code if this was an incident on a subcontractor network;
(viii) Government programs, platforms or systems involved;
(ix) Location(s) of incident;
(x) Date and time the incident was discovered;
(xi) Server names where sensitive information resided at the time of the incident, both at Seller and subcontractor level;
(xii) Description of the Government PII and/or SPII contained within the system;
(xiii) Number of people potentially affected and the estimate or actual number of records exposed and/or contained within the system; and
(xiv) Any additional information relevant to the incident.

(g) *Sensitive Information Incident Response Requirements.*

(1) All determinations related to sensitive information incidents, including response activities, notifications to affected individuals and/or Federal agencies, and related services (e.g., credit monitoring) will be made in writing by the Contracting Officer in consultation with the Headquarters or Component CIO and Headquarters or Component Privacy Officer.

(2) Seller shall provide full access and cooperation for all activities determined by the Government to be required to ensure an effective incident response, including providing all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents.

(3) Incident response activities determined to be required by the Government may include, but are not limited to, the following:
(i) Inspections,
(ii) Investigations,
(iii) Forensic reviews, and
(iv) Data analyses and processing.

(4) The Government, at its sole discretion, may obtain the assistance from other Federal agencies and/or third-party firms to aid in incident response activities.

(h) *Additional PII and/or SPII Notification Requirements.*

(1) Seller shall have in place procedures and the capability to notify any individual whose PII resided in Seller IT system at the time of the sensitive information incident not later than 5 business days after being directed to notify individuals, unless otherwise approved by the Contracting Officer. The method and content of any notification by Seller shall be coordinated with, and subject to prior written approval by the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, utilizing the *DHS Privacy Incident Handling Guidance*. Seller shall not proceed with notification unless the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, has determined in writing that notification is appropriate.

(2) Subject to Government analysis of the incident and the terms of its instructions to Seller regarding any resulting notification, the notification method may consist of letters to affected individuals sent by first class mail, electronic means, or general public notice, as approved by the Government. Notification may require Seller's use of address verification and/or address location services. At a minimum, the notification shall include:

(i) A brief description of the incident;
(ii) A description of the types of PII and SPII involved;
(iii) A statement as to whether the PII or SPII was encrypted or protected by other means;
(iv) Steps individuals may take to protect themselves;
(v) What Seller and/or the Government are doing to investigate the incident, to mitigate the incident, and to protect against any future incidents; and
(vi) Information identifying who individuals may contact for additional information.

(i) *Credit Monitoring Requirements*. In the event that a sensitive information incident involves PII or SPII, Seller may be required to, as directed by the Contracting Officer:

(1) Provide notification to affected individuals as described above; and/or
(2) Provide credit monitoring services to individuals whose data was under the control of Seller or resided in Seller IT system at the time of the sensitive information incident for a period beginning the date of the incident and extending not less than 18 months from the date the individual is

notified. Credit monitoring services shall be provided from a company with which Seller has no affiliation. At a minimum, credit monitoring services shall include:

(i) Triple credit bureau monitoring;
(ii) Daily customer service;
(iii) Alerts provided to the individual for changes and fraud; and
(iv) Assistance to the individual with enrollment in the services and the use of fraud alerts; and/or

(3) Establish a dedicated call center. Call center services shall include:

(i) A dedicated telephone number to contact customer service within a fixed period;
(ii) Information necessary for registrants/enrollees to access credit reports and credit scores;
(iii) Weekly reports on call center volume, issue escalation (i.e., those calls that cannot be handled by call center staff and must be resolved by call center management or DHS, as appropriate), and other key metrics;
(iv) Escalation of calls that cannot be handled by call center staff to call center management or DHS, as appropriate;
(v) Customized FAQs, approved in writing by the Contracting Officer in coordination with the Headquarters or Component Chief Privacy Officer; and
(vi) Information for registrants to contact customer service representatives and fraud resolution representatives for credit monitoring assistance.

(j) *Certification of Sanitization of Government and Government-Activity-Related Files and Information.* As part of contract closeout, Seller shall submit the certification to the COR and the Contracting Officer following the template provided in *NIST Special Publication 800-88 Guidelines for Media Sanitization*.
(End of clause)

14. AMENDMENTS REQUIRED BY PRIME CONTRACT. Buyer may modify these Supplemental Purchasing Terms and Conditions to add any provisions that are reflected in the Prime Contract or in subsequent modifications to the Prime Contract. Accordingly, Seller agrees that upon the request of Buyer, Seller will negotiate in good faith with Buyer relative to modifications to this Purchase Order to incorporate additional provisions herein or to change provisions hereof, as Buyer may reasonably deem necessary in order to comply with the provisions of the Prime Contract, or with the provisions of amendments to the Prime Contract. If any such modification to this Purchase Order causes an increase or decrease in the cost of, or the time required for, performance of any part of the work under this Purchase Order, an equitable adjustment shall be processed pursuant to the “Changes” clause of this Purchase Order.