SEAPORT NXG CONTRACT NO. N0017819D7888
PRIME CONTRACT FLOWDOWNS

BETWEEN

SUBCONTRACTOR
(Also Referred to as **Subcontractor, Offeror** or **Seller**)

AND

Iron Bow Technologies, LLC
2303 Dulles Station Blvd, Suite 400
Herndon, VA 20171
(Also Referred to as **Prime Contractor** or **Buyer**)

WHERE THE WORDS "CONTRACTING OFFICER" AND "CONTRACTOR" APPEAR IN THE TEXT OF SUCH PROVISIONS, SUCH REFERENCE SHALL MEAN "IRON BOW" AND "SUBCONTRACTOR" RESPECTIVELY. REFERENCES IN SUCH PROVISIONS TO THE "GOVERNMENT" SHALL REMAIN AS STATED EXCEPT WHERE IT IS CLEAR THAT "IRON BOW" SHOULD BE SUBSTITUTED ACCORDINGLY. ALL REFERENCES IN SUCH PROVISIONS TO "CONTRACT" SHALL MEAN THIS SUBCONTRACT. ADDITIONAL OR DIFFERING TERMS, CONDITIONS OR LIMITATIONS OF LIABILITY PROPOSED BY SELLER, WHETHER IN A QUOTE, ACCEPTANCE OR DELIVERY DOCUMENT SHALL HAVE NO EFFECT UNLESS ACCEPTED IN WRITING BY BUYER. IN PARTICULAR, ANY LIMITATION OF LIABILITY OR DISCLAIMER OF WARRANTY IS EXPRESSLY REJECTED.

52.242-15	Stop-Work Order	AUG 1989
52.242-15	Alt I Stop-Work Order (Aug 1989) - Alternate I	APR 1984
52.247-34	F.O.B. Destination	NOV 1991
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	
52.203-7	Anti-Kickback Procedures	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	OCT 2010
52.203-13	Contractor Code of Business Ethics and Conduct	OCT 2015
52.203-14	Display of Hotline Poster(s)	OCT 2015
52.203-16	Preventing Personal Conflicts of Interest	DEC 2011
52.203-17	Contractor Employee Whistleblower Rights and Requirement To Inform Employees of Whistleblower Rights	APR 2014
52.203-19	Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements	JAN 2017
52.204-2	Security Requirements	AUG 1996
52.204-4	Printed or Copied Double-Sided on Postconsumer Fiber Content Paper	MAY 2011
52.204-9	Personal Identity Verification of Contractor Personnel	JAN 2011
52.204-10	Reporting Executive Compensation and First-Tier Subcontract Awards	OCT 2016
52.204-12	Unique Entity Identifier Maintenance	OCT 2016
52.204-13	System for Award Management Maintenance	OCT 2016
52.204-14	Service Contract Reporting Requirements	OCT 2016
52.204-15	Service Contract Reporting Requirements for Indefinite-Delivery Contracts	OCT 2016
52.204-19	Incorporation by Reference of Representations and Certifications.	DEC 2014
52.209-6	Protecting the Government's Interest When Subcontracting With Contractors Debarred, Suspended, or Proposed for Debarment	OCT 2015
52.209-9	Updates of Publicly Available Information Regarding Responsibility Matters	JUL 2013
52.209-10	Prohibition on Contracting With Inverted Domestic Corporations	NOV 2015
52.211-15	Defense Priority And Allocation Requirements	APR 2008
52.215-2	Audit and Records--Negotiation	OCT 2010

52.215-8	Order of Precedence--Uniform Contract Format	OCT 1997
52.215-13	Subcontractor Certified Cost or Pricing Data--Modifications	OCT 2010
52.215-14	Integrity of Unit Prices	OCT 2010
52.215-15	Pension Adjustments and Asset Reversions	OCT 2010
52.215-17	Waiver of Facilities Capital Cost of Money	OCT 1997
52.215-18	Reversion or Adjustment of Plans for Postretirement Benefits (PRB) Other than Pensions	JUL 2005
52.215-19	Notification of Ownership Changes	OCT 1997
52.215-23	Limitations on Pass-Through Charges	OCT 2009
52.216-7	Allowable Cost And Payment	JUN 2013
52.216-8	Fixed Fee	JUN 2011
52.216-10	Incentive Fee	JUN 2011
52.216-16	Incentive Price Revision-Firm Target	OCT 1997
52.216-17	Incentive Price Revision-Successive Targets	
52.219-3	Notice of HUBZone Set-Aside or Sole Source Award	NOV 2011
52.219-4	Notice of Price Evaluation Preference for HUBZone Small Business Concerns	OCT 2014
52.219-8	Utilization of Small Business Concerns	NOV 2016
52.219-9	(Dev) Small Business Subcontracting Plan (Deviation 2018-O0013)	APR 2018
52.219-9	Alt II (Dev) Small Business Subcontracting Plan (Deviation 2016-O0009)- Alternate II	JAN 2017
52.219-14	Limitations On Subcontracting	JAN 2017
52.219-16	Liquidated Damages-Subcontracting Plan	JAN 1999
52.219-17	Section 8(a) Award	JAN 2017
52.219-18	Notification Of Competition Limited To Eligible 8(a) Participants	JAN 2017
52.219-27	Notice of Service-Disabled Veteran-Owned Small Business Set-Aside	NOV 2011
52.219-29	Notice of Set-Aside for, or Sole Source Award to, Economically Disadvantaged Women-Owned Small Business Concerns	DEC 2015
52.222-1	Notice To The Government Of Labor Disputes	FEB 1997
52.222-3	Convict Labor	JUN 2003
52.222-17	Nondisplacement of Qualified Workers	MAY 2014
52.222-21	Prohibition Of Segregated Facilities	APR 2015
52.222-26	Equal Opportunity	SEP 2016
52.222-35	Equal Opportunity for Veterans	OCT 2015
52.222-36	Equal Opportunity for Workers with Disabilities	JUL 2014
52.222-37	Employment Reports on Veterans	FEB 2016
52.222-41	Service Contract Labor Standards	MAY 2014
52.222-42	Statement Of Equivalent Rates For Federal Hires	MAY 2014
52.222-43	Fair Labor Standards Act And Service Contract Labor Standards - Price Adjustment (Multiple Year And Option Contracts)	MAY 2014
52.222-50	Combating Trafficking in Persons	MAR 2015
52.222-54	Employment Eligibility Verification	OCT 2015
52.222-55	Minimum Wages Under Executive Order 13658	DEC 2015
52.223-6	Drug-Free Workplace	MAY 2001
52.223-18	Encouraging Contractor Policies To Ban Text Messaging While Driving	AUG 2011
52.224-1	Privacy Act Notification	APR 1984
52.224-2	Privacy Act	APR 1984
52.225-8	Duty-Free Entry	OCT 2010
52.225-13	Restrictions on Certain Foreign Purchases	JUN 2008
52.226-1	Utilization Of Indian Organizations And Indian-Owned Economic Enterprises	JUN 2000
52.227-1	Authorization and Consent	
52.227-2	Notice And Assistance Regarding Patent And Copyright Infringement	
52.227-3	Patent Indemnity	APR 1984
52.227-10	Filing Of Patent Applications--Classified Subject Matter	
52.227-11	Patent Rights--Ownership By The Contractor	MAY 2014
52.227-13	Patent Rights--Ownership By The Government	DEC 2007
52.228-7	Insurance--Liability To Third Persons	MAR 1996
52.229-3	Federal, State And Local Taxes	FEB 2013
52.230-2	Cost Accounting Standards	OCT 2015
52.230-3	Disclosure And Consistency Of Cost Accounting Practices	OCT 2015
52.230-6	Administration of Cost Accounting Standards	JUN 2010
52.232-1	Payments	APR 1984

52.232-8	Discounts For Prompt Payment	FEB 2002
52.232-9	Limitation On Withholding Of Payments	APR 1984
52.232-11	Extras	APR 1984
52.232-17	Interest	MAY 2014
52.232-18	Availability Of Funds	APR 1984
52.232-20	Limitation Of Cost	APR 1984
52.232-22	Limitation Of Funds	APR 1984
52.232-23	Assignment Of Claims	MAY 2014
52.232-23	Alt I Assignment of Claims (May 2014) - Alternate I	APR 1984
52.232-25	Prompt Payment	JAN 2017
52.232-25	Alt I (DUPLICATE) Prompt Payment (Feb 2002) Alternate I	FEB 2002
52.232-32	Performance-Based Payments	APR 2012
52.232-33	Payment by Electronic Funds Transfer--System for Award Management	JUL 2013
52.232-39	Unenforceability of Unauthorized Obligations	JUN 2013
52.232-40	Providing Accelerated Payments to Small Business Subcontractors	DEC 2013
52.233-1	Disputes	MAY 2014
52.233-3	Protest After Award	AUG 1996
52.233-3	Alt I Protest After Award (Aug 1996) - Alternate I	JUN 1985
52.233-4	Applicable Law for Breach of Contract Claim	OCT 2004
52.237-3	Continuity Of Services	JAN 1991
52.239-1	Privacy or Security Safeguards	AUG 1996
52.242-1	Notice of Intent to Disallow Costs	APR 1984
52.242-3	Penalties for Unallowable Costs	MAY 2014
52.242-4	Certification of Final Indirect Costs	JAN 1997
52.242-13	Bankruptcy	JUL 1995
52.243-1	Alt I Changes--Fixed Price (Aug 1987) - Alternate I	APR 1984
52.243-2	Alt I Changes--Cost-Reimbursement (Aug 1987) - Alternate I	APR 1984
52.243-2	Alt II Changes--Cost Reimbursement (Aug 1987) - Alternate II	APR 1984
52.244-2	Subcontracts	OCT 2010
52.244-5	Competition In Subcontracting	DEC 1996
52.244-6	Subcontracts for Commercial Items	NOV 2017
52.245-1	Government Property	JAN 2017
52.245-9	Use And Charges	APR 2012
52.246-25	Limitation Of Liability--Services	FEB 1997
52.248-1	Value Engineering	OCT 2010
52.249-2	Termination For Convenience Of The Government (Fixed-Price)	APR 2012
52.249-6	Termination (Cost Reimbursement)	MAY 2004
52.249-8	Default (Fixed-Price Supply & Service)	APR 1984
52.249-14	Excusable Delays	APR 1984
52.253-1	Computer Generated Forms	JAN 1991
252.201-7000	Contracting Officer's Representative	DEC 1991
252.203-7000	Requirements Relating to Compensation of Former DoD Officials	SEP 2011
252.203-7001	Prohibition On Persons Convicted of Fraud or Other Defense-Contract-Related Felonies	DEC 2008
252.203-7002	Requirement to Inform Employees of Whistleblower Rights	SEP 2013
252.203-7003	Agency Office of the Inspector General	DEC 2012
252.204-7000	Disclosure Of Information	OCT 2016
252.204-7003	Control Of Government Personnel Work Product	APR 1992
252.204-7005	Oral Attestation of Security Responsibilities	NOV 2001
252.204-7006	Billing Instructions	OCT 2005
252.204-7015	Notice of Authorized Disclosure of Information for Litigation Support	MAY 2016
252.205-7000	Provision Of Information To Cooperative Agreement Holders	DEC 1991
252.209-7004	Subcontracting With Firms That Are Owned or Controlled By The Government of a Country that is a State Sponsor of Terrorism	OCT 2015
252.211-7003	Item Unique Identification and Valuation	MAR 2016
252.211-7007	Reporting of Government-Furnished Property	AUG 2012
252.215-7000	Pricing Adjustments	DEC 2012
252.219-7003	Small Business Subcontracting Plan (DOD Contracts)--Basic	MAR 2016
252.222-7006	Restrictions on the Use of Mandatory Arbitration Agreements	DEC 2010
252.223-7004	Drug Free Work Force	SEP 1988

252.225-7001	Buy American And Balance Of Payments Program-- Basic	DEC 2017
252.225-7002	Qualifying Country Sources As Subcontractors	DEC 2017
252.225-7004	Report of Intended Performance Outside the United States and Canada--Submission after Award	OCT 2015
252.225-7012	Preference For Certain Domestic Commodities	DEC 2017
252.225-7048	Export-Controlled Items	JUN 2013
252.226-7001	Utilization of Indian Organizations and Indian-Owned Economic Enterprises, and Native Hawaiian Small Business Concerns	SEP 2004
252.227-7013	Rights in Technical Data--Noncommercial Items	FEB 2014
252.227-7014	Rights in Noncommercial Computer Software and Noncommercial Computer Software Documentation	FEB 2014
252.227-7015	Technical Data--Commercial Items	FEB 2014
252.227-7016	Rights in Bid or Proposal Information	JAN 2011
252.227-7019	Validation of Asserted Restrictions--Computer Software	SEP 2016
252.227-7025	Limitations on the Use or Disclosure of Government-Furnished Information Marked with Restrictive Legends	MAY 2013
252.227-7027	Deferred Ordering Of Technical Data Or Computer Software	APR 1988
252.227-7030	Technical Data--Withholding Of Payment	MAR 2000
252.227-7037	Validation of Restrictive Markings on Technical Data	SEP 2016
252.227-7038	Patent Rights--Ownership by the Contractor (Large Business)	JUN 2012
252.227-7039	Patents--Reporting Of Subject Inventions	APR 1990
252.232-7003	Electronic Submission of Payment Requests and Receiving Reports	JUN 2012
252.232-7004	DOD Progress Payment Rates	OCT 2014
252.232-7010	Levies on Contract Payments	
252.237-7010	Prohibition on Interrogation of Detainees by Contractor Personnel	JUN 2013
252.239-7001	Information Assurance Contractor Training and Certification	JAN 2008
252.239-7010	Cloud Computing Services	OCT 2016
252.242-7004	Material Management And Accounting System	MAY 2011
252.242-7005	Contractor Business Systems	FEB 2012
252.242-7006	Accounting System Administration	FEB 2012
252.243-7001	Pricing Of Contract Modifications	DEC 1991
252.243-7002	Requests for Equitable Adjustment	DEC 2012
252.244-7000	Subcontracts for Commercial Items	JUN 2013
252.244-7001	Contractor Purchasing System Administration	MAY 2014
252.245-7001	Tagging, Labeling, and Marking of Government-Furnished Property	APR 2012
252.245-7002	Reporting Loss of Government Property	DEC 2017
252.245-7003	Contractor Property Management System Administration	APR 2012
252.245-7004	Reporting, Reutilization, and Disposal	DEC 2017
252.246-7001	Warranty Of Data	MAR 2014
252.246-7001	Alt I Warranty Of Data (Mar 2014) - Alternate I	MAR 2014
252.246-7001	Alt II Warranty Of Data (Mar 2014) - Alternate II	MAR 2014
252.247-7023	Transportation of Supplies by Sea	APR 2014
252.247-7024	Notification Of Transportation Of Supplies By Sea	MAR 2000

52.222-50 COMBATING TRAFFICKING IN PERSONS (MAR 2015) ALTERNATE I (MAR 2015)

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

"Agent" means any individual, including a director, an officer, an employee, or an independent contractor, authorized to act on behalf of the organization.

"Coercion" means—

(1) Threats of serious harm to or physical restraint against any person;

(2) Any scheme, plan, or pattern intended to cause a person to believe that failure to perform an act would result in serious harm to or physical restraint against any person; or

(3) The abuse or threatened abuse of the legal process.

"Commercial sex act" means any sex act on account of which anything of value is given to or received by any person.

"Commercially available off-the-shelf (COTS) item" means--

(1) Any item of supply (including construction material) that is—

(i) A commercial item (as defined in paragraph (1) of the definition at FAR 2.101);

(ii) Sold in substantial quantities in the commercial marketplace; and
(iii) Offered to the Government, under a contract or subcontract at any tier, without modification, in the same form in which it is sold in the commercial marketplace; and
(2) Does not include bulk cargo, as defined in 46 U.S.C. 40102(4), such as agricultural products and petroleum products.
"Debt bondage" means the status or condition of a debtor arising from a pledge by the debtor of his or her personal services or of those of a person under his or her control as a security for debt, if the value of those services as reasonably assessed is not applied toward the liquidation of the debt or the length and nature of those services are not respectively limited and defined.
"Employee" means an employee of the Contractor directly engaged in the performance of work under the contract who has other than a minimal impact or involvement in contract performance.
"Forced labor" means knowingly providing or obtaining the labor or services of a person—
(1) By threats of serious harm to, or physical restraint against, that person or another person;
(2) By means of any scheme, plan, or pattern intended to cause the person to believe that, if the person did not perform such labor or services, that person or another person would suffer serious harm or physical restraint; or
(3) By means of the abuse or threatened abuse of law or the legal process.
"Involuntary servitude" includes a condition of servitude induced by means of—
(1) Any scheme, plan, or pattern intended to cause a person to believe that, if the person did not enter into or continue in such conditions, that person or another person would suffer serious harm or physical restraint; or
(2) The abuse or threatened abuse of the legal process.
"Severe forms of trafficking in persons" means—
(1) Sex trafficking in which a commercial sex act is induced by force, fraud, or coercion, or in which the person induced to perform such act has not attained 18 years of age; or
(2) The recruitment, harboring, transportation, provision, or obtaining of a person for labor or services, through the use of force, fraud, or coercion for the purpose of subjection to involuntary servitude, peonage, debt bondage, or slavery.
"Sex trafficking" means the recruitment, harboring, transportation, provision, or obtaining of a person for the purpose of a commercial sex act.
"Subcontract" means any contract entered into by a subcontractor to furnish supplies or services for performance of a prime contract or a subcontract.
"Subcontractor" means any supplier, distributor, vendor, or firm that furnishes supplies or services to or for a prime contractor or another subcontractor.
"United States" means the 50 States, the District of Columbia, and outlying areas.
(b) *Policy*. The United States Government has adopted a policy prohibiting trafficking in persons including the trafficking-related activities of this clause. Contractors, contractor employees, and their agents shall not—
(1) Engage in severe forms of trafficking in persons during the period of performance of the contract;
(2) Procure commercial sex acts during the period of performance of the contract;
(3) Use forced labor in the performance of the contract;
(4) Destroy, conceal, confiscate, or otherwise deny access by an employee to the employee's identity or immigration documents, such as passports or drivers' licenses, regardless of issuing authority;
(5)(i) Use misleading or fraudulent practices during the recruitment of employees or offering of employment, such as failing to disclose, in a format and language accessible to the worker, basic information or making material misrepresentations during the recruitment of employees regarding the key terms and conditions of employment, including wages and fringe benefits, the location of work, the living conditions, housing and associated costs (if employer or agent provided or arranged), any significant cost to be charged to the employee, and, if applicable, the hazardous nature of the work;
(ii) Use recruiters that do not comply with local labor laws of the country in which the recruiting takes place;
(6) Charge employees recruitment fees;
(7)(i) Fail to provide return transportation or pay for the cost of return transportation upon the end of employment--
(A) For an employee who is not a national of the country in which the work is taking place and who was brought into that country for the purpose of working on a U.S. Government contract or subcontract (for portions of contracts performed outside the United States); or
(B) For an employee who is not a United States national and who was brought into the United States for the purpose

of working on a U.S. Government contract or subcontract, if the payment of such costs is required under existing temporary worker programs or pursuant to a written agreement with the employee (for portions of contracts performed inside the United States); except that--
(ii) The requirements of paragraphs (b)(7)(i) of this clause shall not apply to an employee who is--
(A) Legally permitted to remain in the country of employment and who chooses to do so; or
(B) Exempted by an authorized official of the contracting agency from the requirement to provide return transportation or pay for the cost of return transportation;
(iii) The requirements of paragraph (b)(7)(i) of this clause are modified for a victim of trafficking in persons who is seeking victim services or legal redress in the country of employment, or for a witness in an enforcement action related to trafficking in persons. The contractor shall provide the return transportation or pay the cost of return transportation in a way that does not obstruct the victim services, legal redress, or witness activity. For example, the contractor shall not only offer return transportation to a witness at a time when the witness is still needed to testify. This paragraph does not apply when the exemptions at paragraph (b)(7)(ii) of this clause apply.
(8) Provide or arrange housing that fails to meet the host country housing and safety standards; or
(9) If required by law or contract, fail to provide an employment contract, recruitment agreement, or other required work document in writing. Such written work document shall be in a language the employee understands. If the employee must relocate to perform the work, the work document shall be provided to the employee at least five days prior to the employee relocating. The employee's work document shall include, but is not limited to, details about work description, wages, prohibition on charging recruitment fees, work location(s), living accommodations and associated costs, time off, roundtrip transportation arrangements, grievance process, and the content of applicable laws and regulations that prohibit trafficking in persons.
(c) *Contractor requirements*. The Contractor shall—
(1) Notify its employees of—
(i) (A) The United States Government's policy prohibiting trafficking in persons described in paragraph (b) of this clause; and
(B) The following directive(s) or notice(s) applicable to employees performing work at the contract place(s) of performance as indicated below:

Document Title	Document may be obtained from:	Applies to performance in/at:
___	___	___
___	___	___
___	___	___

[___ Contracting Officer shall insert title of directive/notice; indicate the document is attached or provide source (such as website link) for obtaining document; and, indicate the contract performance location outside the United States to which the document applies.]
(ii) The actions that will be taken against employees or agents for violations of this policy. Such actions for employees may include, but are not limited to, removal from the contract, reduction in benefits, or termination of employment; and
(2) Take appropriate action, up to and including termination, against employees, agents, or subcontractors that violate the policy in paragraph (b) of this clause.
(d) *Notification*. (1) The Contractor shall inform the Contracting Officer and the agency Inspector General immediately of—
(i) Any credible information it receives from any source (including host country law enforcement) that alleges a Contractor employee, subcontractor, subcontractor employee, or their agent has engaged in conduct that violates the policy in paragraph (b) of this clause (see also 18 U.S.C. 1351, Fraud in Foreign Labor Contracting, and 52.203-13(b)(3)(i)(A), if that clause is included in the solicitation or contract, which requires disclosure to the agency Office of the Inspector General when the Contractor has credible evidence of fraud); and
(ii) Any actions taken against a Contractor employee, subcontractor, subcontractor employee, or their agent pursuant to this clause.
(2) If the allegation may be associated with more than one contract, the Contractor shall inform the contracting

officer for the contract with the highest dollar value.
(e) *Remedies*. In addition to other remedies available to the Government, the Contractor's failure to comply with the requirements of paragraphs (c), (d), (g), (h), or (i) of this clause may result in—
(1) Requiring the Contractor to remove a Contractor employee or employees from the performance of the contract;
(2) Requiring the Contractor to terminate a subcontract;
(3) Suspension of contract payments until the Contractor has taken appropriate remedial action;
(4) Loss of award fee, consistent with the award fee plan, for the performance period in which the Government determined Contractor non-compliance;
(5) Declining to exercise available options under the contract;
(6) Termination of the contract for default or cause, in accordance with the termination clause of this contract; or
(7) Suspension or debarment.
(f) *Mitigating and aggravating factors*. When determining remedies, the Contracting Officer may consider the following:
(1) *Mitigating factors*. The Contractor had a Trafficking in Persons compliance plan or an awareness program at the time of the violation, was in compliance with the plan, and has taken appropriate remedial actions for the violation, that may include reparation to victims for such violations.
(2) Aggravating factors. The Contractor failed to abate an alleged violation or enforce the requirements of a compliance plan, when directed by the Contracting Officer to do so.
(g) *Full cooperation*.
(1) The Contractor shall, at a minimum—
(i) Disclose to the agency Inspector General information sufficient to identify the nature and extent of an offense and the individuals responsible for the conduct;
(ii) Provide timely and complete responses to Government auditors' and investigators' requests for documents;
(iii) Cooperate fully in providing reasonable access to its facilities and staff (both inside and outside the U.S.) to allow contracting agencies and other responsible Federal agencies to conduct audits, investigations, or other actions to ascertain compliance with the Trafficking Victims Protection Act of 2000 (22 U.S.C. chapter 78), E.O. 13627, or any other applicable law or regulation establishing restrictions on trafficking in persons, the procurement of commercial sex acts, or the use of forced labor; and
(iv) Protect all employees suspected of being victims of or witnesses to prohibited activities, prior to returning to the country from which the employee was recruited, and shall not prevent or hinder the ability of these employees from cooperating fully with Government authorities.
(2) The requirement for full cooperation does not foreclose any Contractor rights arising in law, the FAR, or the terms of the contract. It does not—
(i) Require the Contractor to waive its attorney-client privilege or the protections afforded by the attorney work product doctrine;
(ii) Require any officer, director, owner, employee, or agent of the Contractor, including a sole proprietor, to waive his or her attorney client privilege or Fifth Amendment rights; or
(iii) Restrict the Contractor from—
(A) Conducting an internal investigation; or
(B) Defending a proceeding or dispute arising under the contract or related to a potential or disclosed violation.
(h) *Compliance plan*.
(1) This paragraph (h) applies to any portion of the contract that—
(i) Is for supplies, other than commercially available off-the-shelf items, acquired outside the United States, or services to be performed outside the United States; and
(ii) Has an estimated value that exceeds $500,000.
(2) The Contractor shall maintain a compliance plan during the performance of the contract that is appropriate—
(i) To the size and complexity of the contract; and
(ii) To the nature and scope of the activities to be performed for the Government, including the number of non-United States citizens expected to be employed and the risk that the contract or subcontract will involve services or supplies susceptible to trafficking in persons.
(3) *Minimum requirements*. The compliance plan must include, at a minimum, the following:
(i) An awareness program to inform contractor employees about the Government's policy prohibiting trafficking related activities described in paragraph (b) of this clause, the activities prohibited, and the actions that will be taken

against the employee for violations. Additional information about Trafficking in Persons and examples of awareness programs can be found at the Web site for the Department of State's Office to Monitor and Combat Trafficking in Persons at http://www.state.gov/j/tip/.
(ii) A process for employees to report, without fear of retaliation, activity inconsistent with the policy prohibiting trafficking in persons, including a means to make available to all employees the hotline phone number of the Global Human Trafficking Hotline at 1-844-888-FREE and its email address at help@befree.org.
(iii) A recruitment and wage plan that only permits the use of recruitment companies with trained employees, prohibits charging recruitment fees to the employee, and ensures that wages meet applicable host-country legal requirements or explains any variance.
(iv) A housing plan, if the Contractor or subcontractor intends to provide or arrange housing, that ensures that the housing meets host-country housing and safety standards.
(v) Procedures to prevent agents and subcontractors at any tier and at any dollar value from engaging in trafficking in persons (including activities in paragraph (b) of this clause) and to monitor, detect, and terminate any agents, subcontracts, or subcontractor employees that have engaged in such activities.
(4) *Posting*.
(i) The Contractor shall post the relevant contents of the compliance plan, no later than the initiation of contract performance, at the workplace (unless the work is to be performed in the field or not in a fixed location) and on the Contractor's Web site (if one is maintained). If posting at the workplace or on the Web site is impracticable, the Contractor shall provide the relevant contents of the compliance plan to each worker in writing.
(ii) The Contractor shall provide the compliance plan to the Contracting Officer upon request.
(5) *Certification*. Annually after receiving an award, the Contractor shall submit a certification to the Contracting Officer that—
(i) It has implemented a compliance plan to prevent any prohibited activities identified at paragraph (b) of this clause and to monitor, detect, and terminate any agent, subcontract or subcontractor employee engaging in prohibited activities; and
(ii) After having conducted due diligence, either—
(A) To the best of the Contractor's knowledge and belief, neither it nor any of its agents, subcontractors, or their agents is engaged in any such activities; or
(B) If abuses relating to any of the prohibited activities identified in paragraph (b) of this clause have been found, the Contractor or subcontractor has taken the appropriate remedial and referral actions.
(i) *Subcontracts*.
(1) The Contractor shall include the substance of this clause, including this paragraph (i), in all subcontracts and in all contracts with agents. The requirements in paragraph (h) of this clause apply only to any portion of the subcontract that—
(A) Is for supplies, other than commercially available off-the-shelf items, acquired outside the United States, or services to be performed outside the United States; and
(B) Has an estimated value that exceeds $500,000.
(2) If any subcontractor is required by this clause to submit a certification, the Contractor shall require submission prior to the award of the subcontract and annually thereafter. The certification shall cover the items in paragraph (h)(5) of this clause.

(End of clause)

252.204-7009 LIMITATIONS ON THE USE OR DISCLOSURE OF THIRD-PARTY CONTRACTOR REPORTED CYBER INCIDENT INFORMATION (OCT 2016)
(a) Definitions. As used in this clause--
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.
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 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/categorylist.html) that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide 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.
(b) Restrictions. The Contractor agrees that the following conditions apply to any information it receives or creates in the performance of this contract that is information obtained from a third-party's reporting of a cyber incident pursuant to DFARS clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting (or derived from such information obtained under that clause):
(1) The Contractor shall access and use the information only for the purpose of furnishing advice or technical assistance directly to the Government in support of the Government's activities related to clause 252.204-7012, and shall not be used for any other purpose.
(2) The Contractor shall protect the information against unauthorized release or disclosure.
(3) The Contractor shall ensure that its employees are subject to use and non-disclosure obligations consistent with this clause prior to the employees being provided access to or use of the information.
(4) The third-party contractor that reported the cyber incident is a third-party beneficiary of the non-disclosure agreement between the Government and Contractor, as required by paragraph (b)(3) of
this clause.
(5) A breach of these obligations or restrictions may subject the Contractor to--
(i) Criminal, civil, administrative, and contractual actions in law and equity for penalties, damages, and other appropriate remedies by the United States; and
(ii) Civil actions for damages and other appropriate remedies by the third party that reported the cyber incident, as a third party beneficiary of this clause.
(c) Subcontracts. The Contractor shall include this clause, including this paragraph (c), in subcontracts, or similar contractual instruments, for services that include support for the Government's activities related to safeguarding covered defense information and cyber incident reporting, including subcontracts for commercial items, without alteration, except to identify the parties.
Information system means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
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.
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.

(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/categorylist.html, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide 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 nonapplicable 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)