(Revised October 21, 2016)

252.204-7000 Disclosure of Information.
As prescribed in 204.404-70(a), use the following clause:

DISCLOSURE OF INFORMATION (OCT 2016)

(a) The Contractor shall not release to anyone outside the Contractor's organization any unclassified information, regardless of medium (e.g., film, tape, document), pertaining to any part of this contract or any program related to this contract, unless—

(1) The Contracting Officer has given prior written approval;

(2) The information is otherwise in the public domain before the date of release; or

(3) The information results from or arises during the performance of a project that involves no covered defense information (as defined in the clause at DFARS 252.204-7012) and has been scoped and negotiated by the contracting activity with the contractor and research performer and determined in writing by the contracting officer to be fundamental research (which by definition cannot involve any covered defense information), in accordance with National Security Decision Directive 189, National Policy on the Transfer of Scientific, Technical and Engineering Information, in effect on the date of contract award and the Under Secretary of Defense (Acquisition, Technology, and Logistics) memoranda on Fundamental Research, dated May 24, 2010, and on Contracted Fundamental Research, dated June 26, 2008 (available at DFARS PGI 204.4).

(b) Requests for approval under paragraph (a)(1) shall identify the specific information to be released, the medium to be used, and the purpose for the release. The Contractor shall submit its request to the Contracting Officer at least 10 business days before the proposed date for release.

(c) The Contractor agrees to include a similar requirement, including this paragraph (c), in each subcontract under this contract. Subcontractors shall submit requests for authorization to release through the prime contractor to the Contracting Officer.

(End of clause)

252.204-7001 Reserved.

252.204-7002 Payment for Subline Items Not Separately Priced.
As prescribed in 204.7104-1(b)(3)(iv), use the following clause:

PAYMENT FOR SUBLINE ITEMS NOT SEPARATELY PRICED (DEC 1991)

(a) If the schedule in this contract contains any contract subline items or exhibit subline items identified as not separately priced (NSP), it means that the unit price for that subline item is included in the unit price of another, related line or subline item.

(b) The Contractor shall not invoice the Government for any portion of a contract line item or exhibit line item which contains an NSP until—

(1) The Contractor has delivered the total quantity of all related contract subline items or exhibit subline items; and

(2) The Government has accepted them.

(c) This clause does not apply to technical data.

(End of clause)

252.204-7003 Control of Government Personnel Work Product.
As prescribed in 204.404-70(b), use the following clause:

CONTROL OF GOVERNMENT PERSONNEL WORK PRODUCT (APR 1992)

The Contractor's procedures for protecting against unauthorized disclosure of information shall not require Department of Defense employees or members of the Armed Forces to relinquish control of their work products, whether classified or not, to the Contractor.

(End of clause)

252.204-7004 Alternate A, System for Award Management.

ALTERNATE A, SYSTEM FOR AWARD MANAGEMENT (FEB 2014)

As prescribed in 204.1105, substitute the following paragraph (a) for paragraph (a) of the provision at FAR 52.204-7:

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

"System for Award Management (SAM) database" means the primary Government repository for contractor information required for the conduct of business with the Government.

"Commercial and Government Entity (CAGE) code" means—

(1) A code assigned by the Defense Logistics Information Service (DLIS) to identify a commercial or Government entity; or

(2) A code assigned by a member of the North Atlantic Treaty Organization that DLIS records and maintains in the CAGE master file. This type of code is known as an "NCAGE code."

"Data Universal Numbering System (DUNS) number" means the 9-digit number assigned by Dun and Bradstreet, Inc. (D&B) to identify unique business entities.

"Data Universal Numbering System +4 (DUNS+4) number" means the DUNS number assigned by D&B plus a 4-character suffix that may be assigned by a business concern. (D&B has no affiliation with this 4-character suffix.) This 4-character suffix may be

assigned at the discretion of the business concern to establish additional SAM records for identifying alternative Electronic Funds Transfer (EFT) accounts (see FAR 32.11) for the same parent concern.

"Registered in the System for Award Management (SAM) database" means that—

(1) The contractor has entered all mandatory information, including the DUNS number or the DUNS+4 number, and Contractor and Government Entity (CAGE) code into the SAM database; and

(2) The contractor has completed the Core Data, Assertions, Representations and Certifications, and Points of Contact sections of the registration in the SAM database;

(3) The Government has validated all mandatory data fields, to include validation of the Taxpayer Identification Number (TIN) with the Internal Revenue Service (IRS). The Contractor will be required to provide consent for TIN validation to the Government as part of the SAM registration process; and

(4) The Government has marked the record "Active."

252.204-7005 Oral Attestation of Security Responsibilities.
As prescribed in 204.404-70(c), use the following clause:

ORAL ATTESTATION OF SECURITY RESPONSIBILITIES (NOV 2001)

(a) Contractor employees cleared for access to Top Secret (TS), Special Access Program (SAP), or Sensitive Compartmented Information (SCI) shall attest orally that they will conform to the conditions and responsibilities imposed by law or regulation on those granted access. Reading aloud the first paragraph of Standard Form 312, Classified Information Nondisclosure Agreement, in the presence of a person designated by the Contractor for this purpose, and a witness, will satisfy this requirement. Contractor employees currently cleared for access to TS, SAP, or SCI may attest orally to their security responsibilities when being briefed into a new program or during their annual refresher briefing. There is no requirement to retain a separate record of the oral attestation.

(b) If an employee refuses to attest orally to security responsibilities, the Contractor shall deny the employee access to classified information and shall submit a report to the Contractor's security activity.

(End of clause)

252.204-7006 Billing Instructions.
As prescribed in 204.7109, use the following clause:

BILLING INSTRUCTIONS (OCT 2005)

When submitting a request for payment, the Contractor shall—

(a) Identify the contract line item(s) on the payment request that reasonably reflect contract work performance; and

(b) Separately identify a payment amount for each contract line item included in the payment request.

(End of clause)

252.204-7007 Alternate A, Annual Representations and Certifications. As prescribed in 204.1202, use the following provision:

ALTERNATE A, ANNUAL REPRESENTATIONS AND CERTIFICATIONS (JAN 2015)

Substitute the following paragraphs (d) and (e) for paragraph (d) of the provision at FAR 52.204-8:

(d)(1) The following representations or certifications in the System for Award Management (SAM) database are applicable to this solicitation as indicated:

(i) 252.209-7003, Reserve Officer Training Corps and Military Recruiting on Campus—Representation. Applies to all solicitations with institutions of higher education.

(ii) 252.216-7008, Economic Price Adjustment—Wage Rates or Material Prices Controlled by a Foreign Government. Applies to solicitations for fixed-price supply and service contracts when the contract is to be performed wholly or in part in a foreign country, and a foreign government controls wage rates or material prices and may during contract performance impose a mandatory change in wages or prices of materials.

(iii) 252.222-7007, Representation Regarding Combating Trafficking in Persons, as prescribed in 222.1771. Applies to solicitations with a value expected to exceed the simplified acquisition threshold.

(iv) 252.225-7042, Authorization to Perform. Applies to all solicitations when performance will be wholly or in part in a foreign country.

(v) 252.225-7049, Prohibition on Acquisition of Commercial Satellite Services from Certain Foreign Entities—Representations. Applies to solicitations for the acquisition of commercial satellite services.

(vi) 252.225-7050, Disclosure of Ownership or Control by the Government of a Country that is a State Sponsor of Terrorism. Applies to all solicitations expected to result in contracts of $150,000 or more.

(vii) 252.229-7012, Tax Exemptions (Italy)—Representation. Applies to solicitations and contracts when contract performance will be in Italy.

(viii) 252.229-7013, Tax Exemptions (Spain)—Representation. Applies to solicitations and contracts when contract performance will be in Spain.

(ix) 252.247-7022, Representation of Extent of Transportation by Sea. Applies to all solicitations except those for direct purchase of ocean transportation

services or those with an anticipated value at or below the simplified acquisition threshold.

(2) The following representations or certifications in SAM are applicable to this solicitation as indicated by the Contracting Officer: *[Contracting Officer check as appropriate.]*

___ (i) 252.209-7002, Disclosure of Ownership or Control by a Foreign Government.

___ (ii) 252.225-7000, Buy American—Balance of Payments Program Certificate.

___ (iii) 252.225-7020, Trade Agreements Certificate.

___ Use with Alternate I.

___ (iv) 252.225-7031, Secondary Arab Boycott of Israel.

___ (v) 252.225-7035, Buy American—Free Trade Agreements—Balance of Payments Program Certificate.

___ Use with Alternate I.

___ Use with Alternate II.

___ Use with Alternate III.

___Use with Alternate IV.

___ Use with Alternate V.

(e) The offeror has completed the annual representations and certifications electronically via the SAM website at https://www.acquisition.gov/. After reviewing the SAM database information, the offeror verifies by submission of the offer that the representations and certifications currently posted electronically that apply to this solicitation as indicated in FAR 52.204-8(c) and paragraph (d) of this provision have been entered or updated within the last 12 months, are current, accurate, complete, and applicable to this solicitation (including the business size standard applicable to the NAICS code referenced for this solicitation), as of the date of this offer, and are incorporated in this offer by reference (see FAR 4.1201); except for the changes identified below *[offeror to insert changes, identifying change by provision number, title, date]*. These amended representation(s) and/or certification(s) are also incorporated in this offer and are current, accurate, and complete as of the date of this offer.

FAR/DFARS Provision #	Title	Date	Change

Any changes provided by the offeror are applicable to this solicitation only, and do not result in an update to the representations and certifications located in the SAM

database.

(End of provision)

252.204-7008 Compliance with Safeguarding Covered Defense Information Controls.
As prescribed in 204.7304(a), use the following provision:

COMPLIANCE WITH SAFEGUARDING COVERED DEFENSE INFORMATION CONTROLS (OCT 2016)

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

"Controlled technical information," "covered contractor information system," "covered defense information," "cyber incident," "information system," and "technical information" are defined in clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting.

(b) The security requirements required by contract clause 252.204-7012, shall be implemented for all covered defense information on all covered contractor information systems that support the performance of this contract.

(c) For covered contractor information systems that are not part of an information technology service or system operated on behalf of the Government (see 252.204-7012(b)(2)—

(1) By submission of this offer, the Offeror represents that it will implement the security requirements specified by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" (see http://dx.doi.org/10.6028/NIST.SP.800-171) that are in effect at the time the solicitation is issued or as authorized by the contracting officer not later than December 31, 2017.

(2)(i) If the Offeror proposes to vary from any of the security requirements specified by NIST SP 800-171 that are in effect at the time the solicitation is issued or as authorized by the Contracting Officer, the Offeror shall submit to the Contracting Officer, for consideration by the DoD Chief Information Officer (CIO), a written explanation of—

(A) Why a particular security requirement is not applicable; or

(B) How an alternative but equally effective, security measure is used to compensate for the inability to satisfy a particular requirement and achieve equivalent protection.

(ii) An authorized representative of the DoD CIO will adjudicate offeror requests to vary from NIST SP 800-171 requirements in writing prior to contract award. Any accepted variance from NIST SP 800-171 shall be incorporated into the resulting contract.

(End of provision)

252.204-7009 Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information.
As prescribed in 204.7304(b), use the following clause:

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/category-list.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.

"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.

(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.

(End of clause)

252.204-7010 Requirement for Contractor to Notify DoD if the Contractor's Activities are Subject to Reporting Under the U.S.-International Atomic Energy Agency Additional Protocol.

As prescribed in 204.470-3, use the following clause:

REQUIREMENT FOR CONTRACTOR TO NOTIFY DOD IF THE CONTRACTOR'S ACTIVITIES ARE SUBJECT TO REPORTING UNDER THE U.S.-INTERNATIONAL ATOMIC ENERGY AGENCY ADDITIONAL PROTOCOL (JAN 2009)

(a) If the Contractor is required to report any of its activities in accordance with Department of Commerce regulations (15 CFR Part 781 *et seq*.) or Nuclear Regulatory Commission regulations (10 CFR Part 75) in order to implement the declarations required by the U.S.-International Atomic Energy Agency Additional Protocol (U.S.-IAEA AP), the Contractor shall—

(1) Immediately provide written notification to the following DoD Program Manager:

[Contracting Officer to insert Program Manager's name, mailing address, e-mail address, telephone number, and facsimile number];

(2) Include in the notification—

(i) Where DoD contract activities or information are located relative to the activities or information to be declared to the Department of Commerce or the Nuclear Regulatory Commission; and

(ii) If or when any current or former DoD contract activities and the activities to be declared to the Department of Commerce or the Nuclear Regulatory Commission have been or will be co-located or located near enough to one another to result in disclosure of the DoD activities during an IAEA inspection or visit; and

(3) Provide a copy of the notification to the Contracting Officer.

(b) After receipt of a notification submitted in accordance with paragraph (a) of this clause, the DoD Program Manager will—

(1) Conduct a security assessment to determine if and by what means access may be granted to the IAEA; or

(2) Provide written justification to the component or agency treaty office for a national security exclusion, in accordance with DoD Instruction 2060.03, Application of the National Security Exclusion to the Agreements Between the United States of America and the International Atomic Energy Agency for the Application of Safeguards in the United States of America. DoD will notify the Contractor if a national security exclusion is applied at the Contractor's location to prohibit access by the IAEA.

(c) If the DoD Program Manager determines that a security assessment is required—

(1) DoD will, at a minimum—

(i) Notify the Contractor that DoD officials intend to conduct an assessment of vulnerabilities to IAEA inspections or visits;

(ii) Notify the Contractor of the time at which the assessment will be conducted, at least 30 days prior to the assessment;

(iii) Provide the Contractor with advance notice of the credentials of the DoD

officials who will conduct the assessment; and

(iv) To the maximum extent practicable, conduct the assessment in a manner that does not impede or delay operations at the Contractor's facility; and

(2) The Contractor shall provide access to the site and shall cooperate with DoD officials in the assessment of vulnerabilities to IAEA inspections or visits.

(d) Following a security assessment of the Contractor's facility, DoD officials will notify the Contractor as to—

(1) Whether the Contractor's facility has any vulnerabilities where potentially declarable activities under the U.S.-IAEA AP are taking place;

(2) Whether additional security measures are needed; and

(3) Whether DoD will apply a national security exclusion.

(e) If DoD applies a national security exclusion, the Contractor shall not grant access to IAEA inspectors.

(f) If DoD does not apply a national security exclusion, the Contractor shall apply managed access to prevent disclosure of program activities, locations, or information in the U.S. declaration.

(g) The Contractor shall not delay submission of any reports required by the Department of Commerce or the Nuclear Regulatory Commission while awaiting a DoD response to a notification provided in accordance with this clause.

(h) The Contractor shall incorporate the substance of this clause, including this paragraph (h), in all subcontracts that are subject to the provisions of the U.S.-IAEA AP.

(End of clause)

252.204-7011 Alternative Line Item Structure.
As prescribed in 204.7109(b), insert the following provision:

ALTERNATIVE LINE ITEM STRUCTURE (SEP 2011)

(a) Line items are the basic structural elements in a solicitation or contract that provide for the organization of contract requirements to facilitate pricing, delivery, inspection, acceptance and payment. Line items are organized into contract line items, subline items, and exhibit line items. Separate line items should be established to account for separate pricing, identification (see section 211.274 of the Defense Federal Acquisition Regulation Supplement), deliveries, or funding. The Government recognizes that the line item structure in this solicitation may not conform to every offeror's practices. Failure to correct these issues can result in difficulties in accounting for deliveries and processing payments. Therefore, offerors are invited to propose an alternative line item structure for items on which bids, proposals, or quotes are requested in this solicitation to ensure that the resulting contract structure is

economically and administratively advantageous to the Government and the Contractor.

(b) If an alternative line item structure is proposed, the structure must be consistent with subpart 204.71 of the Defense Federal Acquisition Regulation Supplement and PGI 204.71. A sample line item structure and a proposed alternative structure are as follows:

Solicitation:

ITEM NO.	SUPPLIES/SERVICE	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0001	Computer, Desktop with CPU, Monitor, Keyboard and Mouse	20	EA		

Alternative line item structure offer where monitors are shipped separately:

ITEM NO.	SUPPLIES/SERVICE	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0001	Computer, Desktop with CPU, Keyboard and Mouse	20	EA		
0002	Monitor	20	EA		

(End of provision)

252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting.

As prescribed in 204.7304(c), use the following clause:

SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING (OCT 2016)

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

"Adequate security" means protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information.

"Compromise" means disclosure of information to unauthorized persons, or a violation of the security policy of a system, in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object, or the copying of information to unauthorized media may have occurred.

"Contractor attributional/proprietary information" means information that identifies the contractor(s), whether directly or indirectly, by the grouping of information that can be traced back to the contractor(s) (e.g., program description, facility locations), personally identifiable information, as well as trade secrets, commercial or financial

information, or other commercially sensitive information that is not customarily shared outside of the company.

"Controlled technical information" means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information would meet the criteria, if disseminated, for distribution statements B through F using the criteria set forth in DoD Instruction 5230.24, Distribution Statements on Technical Documents. The term does not include information that is lawfully publicly available without restrictions.

"Covered contractor information system" means an unclassified information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits covered defense information.

"Covered defense information" means unclassified controlled technical information or other information, as described in the Controlled Unclassified Information (CUI) Registry at http://www.archives.gov/cui/registry/category-list.html, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and 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)

252.204-7013 Limitations on the Use or Disclosure of Information by Litigation Support Offerors.

As prescribed in 204.7403(a), use the following provision. If the solicitation is a request for quotations, the terms "quotation" and "Quoter" may be substituted for "offer" and "Offeror".

LIMITATIONS ON THE USE OR DISCLOSURE OF INFORMATION BY LITIGATION SUPPORT OFFERORS (MAY 2016)

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

"Computer software" means computer programs, source code, source code listings, object code listings, design details, algorithms, processes, flow charts, formulae, and related material that would enable the software to be reproduced, recreated, or recompiled. Computer software does not include computer data bases or computer software documentation.

"Litigation information" means any information, including sensitive information, that is furnished to the contractor by or on behalf of the Government, or that is generated or obtained by the contractor in the performance of litigation support under a contract. The term does not include information that is lawfully, publicly available without restriction, including information contained in a publicly available solicitation.

"Litigation support" means administrative, technical, or professional services provided in support of the Government during or in anticipation of litigation.

"Sensitive information" means controlled unclassified information of a commercial, financial, proprietary, or privileged nature. The term includes technical data and computer software, but does not include information that is lawfully, publicly available without restriction.

"Technical data" means recorded information, regardless of the form or method of the recording, of a scientific or technical nature (including computer software documentation). The term does not include computer software or data incidental to contract administration, such as financial and/or management information.

(b) *Limitations on use or disclosure of litigation information.* Notwithstanding any other provision of this solicitation, by submission of its offer, the Offeror agrees and acknowledges that—

(1) All litigation information will be accessed and used for the sole purpose of providing litigation support;

(2) The Offeror will take all precautions necessary to prevent unauthorized disclosure of litigation information;

(3) The litigation information shall not be used by the Offeror to compete against a third party for Government or nongovernment contracts; and

(4) Upon completion of the authorized litigation support activities, the Offeror will destroy or return to the Government at the request of the Contracting Officer all litigation information in its possession.

(c) *Indemnification and creation of third party beneficiary rights.* By submission of its offer, the Offeror agrees—

(1) To indemnify and hold harmless the Government, its agents, and employees from any claim or liability, including attorneys' fees, court costs, and expenses, arising out of, or in any way related to, the misuse or unauthorized modification, reproduction, release, performance, display, or disclosure of any litigation information; and

(2) That any third party holding proprietary rights or any other legally protectable interest in any litigation information, in addition to any other rights it may have, is a third party beneficiary who shall have a right of direct action against the Offeror, and against any person to whom the Offeror has released or disclosed such litigation information, for any such unauthorized use or disclosure of such information.

(d) *Offeror employees.* By submission of its offer, the Offeror agrees to ensure that its employees are subject to use and nondisclosure obligations consistent with this provision prior to the employees being provided access to or use of any litigation information covered by this provision.

(End of provision)

252.204-7014 Limitations on the Use or Disclosure of Information by Litigation Support Contractors.

As prescribed in 204.7403(b), use the following clause:

LIMITATIONS ON THE USE OR DISCLOSURE OF INFORMATION BY LITIGATION SUPPORT CONTRACTORS (MAY 2016)

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

"Computer software" means computer programs, source code, source code listings, object code listings, design details, algorithms, processes, flow charts, formulae, and related material that would enable the software to be reproduced, recreated, or recompiled. Computer software does not include computer data bases or computer software documentation.

"Litigation information" means any information, including sensitive information, that is furnished to the contractor by or on behalf of the Government, or that is generated or obtained by the contractor in the performance of litigation support work under a contract. The term does not include information that is lawfully, publicly available without restriction, including information contained in a publicly available solicitation.

"Litigation support" means administrative, technical, or professional services provided in support of the Government during or in anticipation of litigation.

"Litigation support contractor" means a contractor (including its experts, technical consultants, subcontractors, and suppliers) providing litigation support under a contract that contains this clause.

"Sensitive information" means controlled unclassified information of a commercial, financial, proprietary, or privileged nature. The term includes technical data and

computer software, but does not include information that is lawfully, publicly available without restriction.

"Technical data" means recorded information, regardless of the form or method of the recording, of a scientific or technical nature (including computer software documentation). The term does not include computer software or data incidental to contract administration, such as financial and/or management information.

(b) *Limitations on use or disclosure of litigation information.* Notwithstanding any other provision of this contract, the Contractor shall—

(1) Access and use litigation information only for the purpose of providing litigation support under this contract;

(2) Not disclose litigation information to any entity outside the Contractor's organization unless, prior to such disclosure the Contracting Officer has provided written consent to such disclosure;

(3) Take all precautions necessary to prevent unauthorized disclosure of litigation information;

(4) Not use litigation information to compete against a third party for Government or nongovernment contracts; and

(5) Upon completion of the authorized litigation support activities, destroy or return to the Government at the request of the Contracting Officer all litigation information in its possession.

(c) Violation of paragraph (b)(1), (b)(2), (b)(3), (b)(4), or (b)(5) of this clause, is a basis for the Government to terminate this contract.

(d) *Indemnification and creation of third party beneficiary rights.* The Contractor agrees—

(1) To indemnify and hold harmless the Government, its agents, and employees from any claim or liability, including attorneys' fees, court costs, and expenses, arising out of, or in any way related to, the misuse or unauthorized modification, reproduction, release, performance, display, or disclosure of any litigation information; and

(2) That any third party holding proprietary rights or any other legally protectable interest in any litigation information, in addition to any other rights it may have, is a third party beneficiary under this contract who shall have a right of direct action against the Contractor, and against any person to whom the Contractor has released or disclosed such litigation information, for any such unauthorized use or disclosure of such information.

(e) *Contractor employees.* The Contractor shall ensure that its employees are subject to use and nondisclosure obligations consistent with this clause prior to the employees being provided access to or use of any litigation information covered by this clause.

(f) *Flowdown.* Include the substance of this clause, including this paragraph (f), in

all subcontracts, including subcontracts for commercial items.

(End of clause)

252.204-7015 Notice of Authorized Disclosure of Information for Litigation Support.
As prescribed in 204.7403(c), use the following clause:

NOTICE OF AUTHORIZED DISCLOSURE OF INFORMATION FOR LITIGATION SUPPORT (MAY 2016)

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

"Computer software" means computer programs, source code, source code listings, object code listings, design details, algorithms, processes, flow charts, formulae, and related material that would enable the software to be reproduced, recreated, or recompiled. Computer software does not include computer data bases or computer software documentation.

"Litigation support" means administrative, technical, or professional services provided in support of the Government during or in anticipation of litigation.

"Litigation support contractor" means a contractor (including its experts, technical consultants, subcontractors, and suppliers) providing litigation support under a contract that contains the clause at 252.204-7014, Limitations on the Use or Disclosure of Information by Litigation Support Contractors.

"Sensitive information" means controlled unclassified information of a commercial, financial, proprietary, or privileged nature. The term includes technical data and computer software, but does not include information that is lawfully, publicly available without restriction.

"Technical data" means recorded information, regardless of the form or method of the recording, of a scientific or technical nature (including computer software documentation). The term does not include computer software or data incidental to contract administration, such as financial and/or management information.

(b) *Notice of authorized disclosures.* Notwithstanding any other provision of this solicitation or contract, the Government may disclose to a litigation support contractor, for the sole purpose of litigation support activities, any information, including sensitive information, received--

(1) Within or in connection with a quotation or offer; or

(2) In the performance of or in connection with a contract.

(c) *Flowdown.* Include the substance of this clause, including this paragraph (c), in all subcontracts, including subcontracts for commercial items.

(End of clause)