

Collection Instruments
OMB Control Number 0704-0478

PART 252—SOLICITATION PROVISIONS AND CONTRACT CLAUSES

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)

252.204-7012 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 (DEC 2019)

(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 <https://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 <https://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 <https://public.cyber.mil/eca/>.

(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)

* * * * *

252.239-7009 Representation of Use of Cloud Computing.

As prescribed in [239.7604\(a\)](#), use the following provision:

REPRESENTATION OF USE OF CLOUD COMPUTING (SEP 2015)

(a) *Definition.* "Cloud computing," as used in this provision, means a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This includes other commercial terms, such as on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. It also includes commercial offerings for software-as-a-service, infrastructure-as-a-service, and platform-as-a-service.

(b) The Offeror shall indicate by checking the appropriate blank in paragraph (c) of this provision whether the use of cloud computing is anticipated under the resultant contract.

(c) *Representation.* The Offeror represents that it—

_____ Does anticipate that cloud computing services will be used in the performance of any contract or subcontract resulting from this solicitation.

_____ Does not anticipate that cloud computing services will be used in the performance of any contract or subcontract resulting from this solicitation.

(End of provision)

252.239-7010 Cloud Computing Services.

As prescribed in [239.7604\(b\)](#), use the following clause:

CLLOUD COMPUTING SERVICES (OCT 2016)

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

“Authorizing official,” as described in DoD Instruction 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT), means the senior Federal official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

“Cloud computing” means a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This includes other commercial terms, such as on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. It also includes commercial offerings for software-as-a-service, infrastructure-as-a-service, and platform-as-a-service.

“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.

“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.

“Government data” means any information, document, media, or machine readable material regardless of physical form or characteristics, that is created or obtained by the Government in the course of official Government business.

“Government-related data” means any information, document, media, or machine readable material regardless of physical form or characteristics that is created or obtained by a contractor through the storage, processing, or communication of Government data. This does not include contractor’s business records e.g. financial records, legal records etc. or data such as operating procedures, software coding or algorithms that are not uniquely applied to the Government data.

“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 not limited to, magnetic tapes, optical disks, magnetic disks, large-scale integration memory chips, and printouts onto which information is recorded, stored, or printed within an information system.

“Spillage” security incident that results in the transfer of classified or controlled unclassified information onto an information system not accredited (i.e., authorized) for the appropriate security level.

(b) *Cloud computing security requirements.* The requirements of this clause are applicable when using cloud computing to provide information technology services in the performance of the contract.

(1) If the Contractor indicated in its offer that it “does not anticipate the use of cloud computing services in the performance of a resultant contract,” in response to provision [252.239-7009](#), Representation of Use of Cloud Computing, and after the award of this contract, the Contractor proposes to use cloud computing services in the performance of the contract, the Contractor shall obtain approval from the Contracting Officer prior to utilizing cloud computing services in performance of the contract.

(2) The Contractor shall implement and maintain administrative, technical, and physical safeguards and controls with the security level and services required in accordance with the Cloud Computing Security Requirements Guide (SRG) (version in effect at the time the solicitation is issued or as authorized by the Contracting Officer) found at http://iase.disa.mil/cloud_security/Pages/index.aspx, unless notified by the Contracting Officer that this requirement has been waived by the DoD Chief Information Officer.

(3) The Contractor shall maintain within the United States or outlying areas all Government data that is not physically located on DoD premises, unless the Contractor receives written notification from the Contracting Officer to use another location, in accordance with DFARS [239.7602-2\(a\)](#).

(c) *Limitations on access to, and use and disclosure of Government data and Government-related data.*

(1) The Contractor shall not access, use, or disclose Government data unless specifically authorized by the terms of this contract or a task order or delivery order issued hereunder.

(i) If authorized by the terms of this contract or a task order or delivery order issued hereunder, any access to, or use or disclosure of, Government data shall only be for purposes specified in this contract or task order or delivery order.

(ii) The Contractor shall ensure that its employees are subject to all such access, use, and disclosure prohibitions and obligations.

(iii) These access, use, and disclosure prohibitions and obligations shall survive the expiration or termination of this contract.

(2) The Contractor shall use Government-related data only to manage the operational environment that supports the Government data and for no other purpose unless otherwise permitted with the prior written approval of the Contracting Officer.

(d) *Cloud computing services cyber incident reporting.* The Contractor shall report all cyber incidents that are related to the cloud computing service provided under this contract. Reports shall be submitted to DoD via <http://dibnet.dod.mil/>.

(e) *Malicious software.* The Contractor or subcontractors that discover and isolate malicious software in connection with a reported cyber incident shall submit the malicious software in accordance with instructions provided by the Contracting Officer.

(f) *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 the cyber incident report (see paragraph (d) 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.

(g) *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.

(h) *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 (f) of this clause.

(i) *Records management and facility access.*

(1) The Contractor shall provide the Contracting Officer all Government data and Government-related data in the format specified in the contract.

(2) The Contractor shall dispose of Government data and Government-related data in accordance with the terms of the contract and provide the confirmation of disposition to the Contracting Officer in accordance with contract closeout procedures.

(3) The Contractor shall provide the Government, or its authorized representatives, access to all Government data and Government-related data, access to contractor personnel involved in performance of the contract, and physical access to any Contractor facility with Government data, for the purpose of audits, investigations, inspections, or other similar activities, as authorized by law or regulation.

(j) *Notification of third party access requests.* The Contractor shall notify the Contracting Officer promptly of any requests from a third party for access to

Government data or Government-related data, including any warrants, seizures, or subpoenas it receives, including those from another Federal, State, or local agency. The Contractor shall cooperate with the Contracting Officer to take all measures to protect Government data and Government-related data from any unauthorized disclosure.

(k) *Spillage*. Upon notification by the Government of a spillage, or upon the Contractor's discovery of a spillage, the Contractor shall cooperate with the Contracting Officer to address the spillage in compliance with agency procedures.

(l) *Subcontracts*. The Contractor shall include this clause, including this paragraph (l), in all subcontracts that involve or may involve cloud services, including subcontracts for commercial items.

(End of clause)