



## **Flow Down Attachment**

### **FDA N1004-24-P-QA63**

**Business Unit:** Naval Sustainment  
**Customer Contract Number:** N00104-24-P-QA63  
**Prime Contract Number:** N00104-24-P-QA63  
**Task Order/Delivery Order Number:** Standalone Contract  
**Modification Number:** Basic  
**DPAS Rating:** DO-A3  
**DUNS Number:** 117913473  
**Date of Creation:** 27 Nov 2023

*The following customer contract requirements apply to this Purchase Order to the extent indicated below and are hereby incorporated into the Purchase Order by full text or by reference with the same force and effect as if they were given in full text. Upon Seller's request, Buyer's Purchasing Representative will make their full text available. Also, the full text of a FAR or DFARS provision or clause may be accessed electronically at these addresses: <http://farsite.hill.af.mil/> or <https://www.acquisition.gov/far/>:*

In all provisions and clauses listed herein, terms shall be revised to suitably identify the party to establish Seller's obligations to Buyer and to the Government, and to enable Buyer to meet its obligations under the prime contract. Without limiting the generality of the foregoing, and except where further clarified or modified below, the term "Government" and equivalent phrases shall mean "Buyer", the term "Contracting Officer" shall mean "Buyer's Purchasing Representative", the term "Contractor" or "Offeror" shall mean "Seller", "Subcontractor" shall mean "Seller's Subcontractor" under this Purchase Order, and the term "Contract" shall mean this "Purchase Order". For the avoidance of doubt, the words "Government" and "Contracting Officer" do not change: (1) when a right, act, authorization or obligation can be granted or performed only by the Government or the prime contract Contracting Officer or duly authorized representative, such as in FAR 52.227-1 and FAR 52.227-2 or (2) when title to property is to be transferred directly to the Government. Seller shall incorporate into each lower tier contract issued in support of this Purchase Order all applicable FAR and DFARS provisions and clauses in accordance with the flow down requirements specified in such clauses. Nothing in this Purchase Order grants Seller a direct right of action against the Government. If any of the following FAR or DFARS clauses do not apply to this Purchase Order, such clauses are considered to be self-deleting.

**CLAUSES INCORPORATED BY REFERENCE:**



Clause Number	Clause Date	Title	Applicability (Reference to 'Purchase Orders' includes underlying Solicitations)
52.204-9	Jan 2011	Personal Identity Verification of Contractor Personnel	Applicable to all Orders when Seller's employees are required to have routine physical access to a Federally-controlled facility and / or routine access to a Federally-controlled information system.
52.204-10	Jun 2020	Reporting Executive Compensation and First-Tier Subcontract Awards	Applicable to all Orders when the Buyer is the Prime Contractor and the Order exceeds \$30,000. Substitution of the parties is not applicable to this clause. Seller shall report to Buyer the information required under the clause.
52.204-23	Nov-21	Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities	Applicable to all Orders, including for commercial products or commercial services.
52.204-25	Nov 2021	Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment	Applicable to all Orders, including subcontracts for the acquisition of commercial products or commercial services.
52.211-5	Aug 2000	Material Requirements	Applicable to Orders for supplies that are not Commercial Items.
52.222-19	Dec 2022	Child Labor-Cooperation with Authorities and Remedies	Applicable to Orders for the acquisition of supplies that are expected to exceed the micro-purchase thresholds.



52.222-20	Jun 2020	Contracts for Materials, Supplies, Articles, and Equipment (Jun 2020)	Applicable to Orders over \$15,000 for the manufacture or furnishing of materials, supplies, articles or equipment.
52.222-21	Apr 2015	Prohibition of Segregated Facilities	Applicable to all Orders, including for Commercial Items pursuant to 52.244-6. Foreign Sellers: Applicable to Orders except to the extent that work under the Order will be performed outside the United States or by employees that are not recruited within the United States to work on the Order. "United States", as used in this parenthetical, means the 50 States, the District of Columbia, Puerto Rico, the Northern Mariana Islands, American Samoa, Guam, the U.S. Virgin Islands, and Wake Island.
52.222-26	Sep 2016	Equal Opportunity	Applicable to all Orders, including for Commercial Items pursuant to 52.244-6, that are not exempted by the rules, regulations, or orders of the Secretary of Labor issued under Executive Order 11246, as amended. Foreign Sellers: Applicable to Orders except to the extent that work under the Order will be performed outside the United States or by employees that are not recruited within the United States to work on the Order. "United States", as used in this parenthetical, means the 50 States, the District of Columbia, Puerto Rico, the Northern Mariana Islands, American Samoa, Guam, the U.S. Virgin Islands, and Wake Island.
52.222-50	Nov 2021	Combating Trafficking in Persons	Applicable to all Orders, including for Commercial Items pursuant to 52.244-6, except that the requirements in paragraph (h) of the clause apply only to (i) supplies that are other than commercially available off-the-shelf items that are acquired outside the United States, or for services to be performed outside the United States, and (ii) that exceed \$550,000 in value.



52.223-18	Jun 2020	Encouraging Contractor Policies To Ban Text Messaging While Driving	Applicable to all Orders over the Micro-Purchase Threshold.
52.244-6	Nov 2023	Subcontracts for Commercial Items	Applicable to all Orders.
52.245-1	Sep 2021	Government Property	Applicable to all Orders when Government property is acquired or furnished (see PT-001).
52.245-9	Apr 2012	Use and Charges	Applicable to all Orders when Government property is acquired or furnished (see PT-001).
252.203-7000	Sep 2011	Requirements Relating to Compensation of Former DoD Officials	Applicable to all Orders.
252.204-7012	Dec-19	Safeguarding Covered Defense Information and Cyber Incident Reporting	Applicable to all Orders for operationally critical support, or for which Order performance will involve covered defense information.
252.204-7015	Jan 2023	Notice of Authorized Disclosure of Information for Litigation Support	Applicable to all Orders.
252.204-7018	Jan 2023	Prohibition on the Acquisition of Covered Defense Telecommunications Equipment or Services	Applicable to all Orders including those for the acquisition of Commercial Items.
252.204-7020	Jan 2023	NIST SP 800-171 DoD Assessment Requirements	Applicable to all Orders, including those using FAR part 12 procedures for the acquisition of commercial products and commercial services, except for those that are solely for the acquisition of COTS items.



252.211-7003	Jan 2023	Item Unique Identification and Valuation	Applicable to all Orders. Seller's obligations under this clause are limited to cooperating with Buyer's efforts to comply with this clause, including granting Buyer access to Seller's deliverables at its facilities and to appropriate property records.
252.223-7001	Dec 1991	Hazard Warning Labels	Applicable to all Orders for goods that require submission of hazardous material data sheets. (See FAR 23.302(c))
252.223-7008	Jan 2023	Prohibition of Hexavalent Chromium	Applicable to all Orders, including subcontracts for commercial items, for supplies, maintenance and repair services, or construction materials.
252.225-7001	Jan 2023	Buy American and Balance of Payments Program	Applicable to all Orders except Orders for commercially available off-the-shelf items (COTS) as defined at FAR 2.101. Seller must deliver goods that contain more than 50% United States or Qualifying Country content pursuant to the clause.
252.225-7012	Apr 2022	Preference for Certain Domestic Commodities	Applicable to all Orders, including those using FAR part 12 procedures for the acquisition of commercial items.
252.225-7013	Dec 2022	Duty-Free Entry	Applicable to Orders for the acquisition of (i) Qualifying Country Components (as defined in paragraph (a) of this clause) or (ii) Nonqualifying Country Components (defined in paragraph (a)) for which the Seller estimates that duty will exceed \$200 per unit to be delivered from foreign locations that will be entering into the customs territory of the United States. Information required by paragraphs (j)(2) and (j)(3) of this clause will be made available upon request.
252.225-7016	Jan 2023	Restriction on Acquisition of Ball and Roller Bearings	Applicable to all Orders for Goods that contain ball or roller bearings, except those that are for commercial items.
252.225-7025	Dec 2009	Restriction on Acquisition of Forgings	Applicable to all Orders for forging items or for other items that contain forging items.



252.225-7036	Jan 2023	Buy American—Free Trade Agreements—Balance of Payments Program—Basic	Applicable if the estimated contract value is within the minimum and maximum dollar thresholds in effect at the time of prime contract issuance, unless an exception at FAR 25.401 or DFARS 225.401 applies and the acquisition is of end products in support of operations in Afghanistan.
252.225-7048	Jun 2013	Export-Controlled Items	Applicable to all Orders.
252.244-7000	Jan 2023	Subcontracts for Commercial Items and Commercial Components	Applicable to all Orders.
252.246-7008	Jan 2023	Sources of Electronic Parts	Applicable to all Orders for electronic parts or assemblies containing electronic parts, unless Seller is the original manufacturer.

CLAUSES INCORPORATED IN FULL TEXT:

-----

DFARS 252.211-7003 (Jan 2023) Item Identification and Valuation:

(a) Definitions. As used in this clause—

“Automatic identification device” means a device, such as a reader or interrogator, used to retrieve data encoded on machine-readable media.

“Concatenated unique item identifier” means—

(1) For items that are serialized within the enterprise identifier, the linking together of the unique identifier data elements in order of the issuing agency code, enterprise identifier, and unique serial number within the enterprise identifier; or

(2) For items that are serialized within the original part, lot, or batch number, the linking together of the unique identifier data elements in order of the issuing agency code; enterprise identifier; original part, lot, or batch number; and serial number within the original part, lot, or batch number.

“Data matrix” means a two-dimensional matrix symbology, which is made up of square or, in some cases, round modules arranged within a perimeter finder pattern and uses the Error Checking and Correction 200 (ECC200) specification found within International Standards Organization (ISO)/International Electrotechnical Commission (IEC) 16022.

“Data qualifier” means a specified character (or string of characters) that immediately precedes a data field that defines the general category or intended use of the data that follows.



“DoD recognized unique identification equivalent” means a unique identification method that is in commercial use and has been recognized by DoD. All DoD recognized unique identification equivalents are listed at <https://www.acq.osd.mil/asda/dpc/ce/ds/unique-id.html>.

“DoD item unique identification” means a system of marking items delivered to DoD with unique item identifiers that have machine-readable data elements to distinguish an item from all other like and unlike items. For items that are serialized within the enterprise identifier, the unique item identifier shall include the data elements of the enterprise identifier and a unique serial number. For items that are serialized within the part, lot, or batch number within the enterprise identifier, the unique item identifier shall include the data elements of the enterprise identifier; the original part, lot, or batch number; and the serial number.

“Enterprise” means the entity (e.g., a manufacturer or vendor) responsible for assigning unique item identifiers to items.

“Enterprise identifier” means a code that is uniquely assigned to an enterprise by an issuing agency.

“Government’s unit acquisition cost” means—

(1) For fixed-price type line, subline, or exhibit line items, the unit price identified in the contract at the time of delivery;

(2) For cost-type or undefinitized line, subline, or exhibit line items, the Contractor’s estimated fully burdened unit cost to the Government at the time of delivery; and

(3) For items produced under a time-and-materials contract, the Contractor’s estimated fully burdened unit cost to the Government at the time of delivery.

“Issuing agency” means an organization responsible for assigning a globally unique identifier to an enterprise, as indicated in the Register of Issuing Agency Codes for ISO/IEC 15459, located at [http://www.aimglobal.org/?Reg\\_Authority15459](http://www.aimglobal.org/?Reg_Authority15459).

“Issuing agency code” means a code that designates the registration (or controlling) authority for the enterprise identifier.

“Item” means a single hardware article or a single unit formed by a grouping of subassemblies, components, or constituent parts.

“Lot or batch number” means an identifying number assigned by the enterprise to a designated group of items, usually referred to as either a lot or a batch, all of which were manufactured under identical conditions.

“Machine-readable” means an automatic identification technology media, such as bar codes, contact memory buttons, radio frequency identification, or optical memory cards.

“Original part number” means a combination of numbers or letters assigned by the enterprise at item creation to a class of items with the same form, fit, function, and interface.

“Parent item” means the item assembly, intermediate component, or subassembly that has an embedded item with a unique item identifier or DoD recognized unique identification equivalent.



“Serial number within the enterprise identifier” means a combination of numbers, letters, or symbols assigned by the enterprise to an item that provides for the differentiation of that item from any other like and unlike item and is never used again within the enterprise.

“Serial number within the part, lot, or batch number” means a combination of numbers or letters assigned by the enterprise to an item that provides for the differentiation of that item from any other like item within a part, lot, or batch number assignment.

“Serialization within the enterprise identifier” means each item produced is assigned a serial number that is unique among all the tangible items produced by the enterprise and is never used again. The enterprise is responsible for ensuring unique serialization within the enterprise identifier.

“Serialization within the part, lot, or batch number” means each item of a particular part, lot, or batch number is assigned a unique serial number within that part, lot, or batch number assignment. The enterprise is responsible for ensuring unique serialization within the part, lot, or batch number within the enterprise identifier.

“Type designation” means a combination of letters and numerals assigned by the Government to a major end item, assembly or subassembly, as appropriate, to provide a convenient means of differentiating between items having the same basic name and to indicate modifications and changes thereto.

“Unique item identifier” means a set of data elements marked on items that is globally unique and unambiguous. The term includes a concatenated unique item identifier or a DoD recognized unique identification equivalent.

“Unique item identifier type” means a designator to indicate which method of uniquely identifying a part has been used. The current list of accepted unique item identifier types is maintained at <https://www.acq.osd.mil/asda/dpc/ce/ds/unique-id.html> .

(b) The Contractor shall deliver all items under a contract line, subline, or exhibit line item.

(c) Unique item identifier.

(1) The Contractor shall provide a unique item identifier for the following:

(i) Delivered items for which the Government’s unit acquisition cost is \$5,000 or more, except for the following line items:

Contract Line, Subline, or

Exhibit Line Item Number Item Description

---

---

---

(ii) Items for which the Government’s unit acquisition cost is less than \$5,000 that are identified in the Schedule or the following table:





Contract Line, Subline, or

Exhibit Line Item Number Item Description

---

---

---

(If items are identified in the Schedule, insert "See Schedule" in this table.)

(iii) Subassemblies, components, and parts embedded within delivered items, items with warranty requirements, DoD serially managed reparables and DoD serially managed nonreparables as specified in Attachment Number \_\_\_\_.

(iv) Any item of special tooling or special test equipment as defined in FAR 2.101 that have been designated for preservation and storage for a Major Defense Acquisition Program as specified in Attachment Number \_\_\_\_.

(v) Any item not included in (i), (ii), (iii), or (iv) for which the contractor creates and marks a unique item identifier for traceability.

(2) The unique item identifier assignment and its component data element combination shall not be duplicated on any other item marked or registered in the DoD Item Unique Identification Registry by the contractor.

(3) The unique item identifier component data elements shall be marked on an item using two dimensional data matrix symbology that complies with ISO/IEC International Standard 16022, Information technology – International symbology specification – Data matrix; ECC200 data matrix specification.

(4) Data syntax and semantics of unique item identifiers. The Contractor shall ensure that—

(i) The data elements (except issuing agency code) of the unique item identifier are encoded within the data matrix symbol that is marked on the item using one of the following three types of data qualifiers, as determined by the Contractor:

(A) Application Identifiers (AIs) (Format Indicator 05 of ISO/IEC International Standard 15434), in accordance with ISO/IEC International Standard 15418, Information Technology – EAN/UCC Application Identifiers and Fact Data Identifiers and Maintenance and ANSI MH 10.8.2 Data Identifier and Application Identifier Standard.

(B) Data Identifiers (DIs) (Format Indicator 06 of ISO/IEC International Standard 15434), in accordance with ISO/IEC International Standard 15418, Information Technology – EAN/UCC Application Identifiers and Fact Data Identifiers and Maintenance and ANSI MH 10.8.2 Data Identifier and Application Identifier Standard.

(C) Text Element Identifiers (TEIs) (Format Indicator 12 of ISO/IEC International Standard 15434), in accordance with the Air Transport Association Common Support Data Dictionary; and



(ii) The encoded data elements of the unique item identifier conform to the transfer structure, syntax, and coding of messages and data formats specified for Format Indicators 05, 06, and 12 in ISO/IEC International Standard 15434, Information Technology – Transfer Syntax for High Capacity Automatic Data Capture Media.

(5) Unique item identifier.

(i) The Contractor shall—

(A) Determine whether to—

(1) Serialize within the enterprise identifier;

(2) Serialize within the part, lot, or batch number; or

(3) Use a DoD recognized unique identification equivalent (e.g. Vehicle Identification Number); and

(B) Place the data elements of the unique item identifier (enterprise identifier; serial number; DoD recognized unique identification equivalent; and for serialization within the part, lot, or batch number only: original part, lot, or batch number) on items requiring marking by paragraph (c)(1) of this clause, based on the criteria provided in MIL-STD-130, Identification Marking of U.S. Military Property, latest version;

(C) Label shipments, storage containers and packages that contain uniquely identified items in accordance with the requirements of MIL-STD-129, Military Marking for Shipment and Storage, latest version; and

(D) Verify that the marks on items and labels on shipments, storage containers, and packages are machine readable and conform to the applicable standards. The contractor shall use an automatic identification technology device for this verification that has been programmed to the requirements of Appendix A, MIL-STD-130, latest version.

(ii) The issuing agency code—

(A) Shall not be placed on the item; and

(B) Shall be derived from the data qualifier for the enterprise identifier.

(d) For each item that requires item unique identification under paragraph (c)(1)(i), (ii), or (iv) of this clause or when item unique identification is provided under paragraph (c)(1)(v), in addition to the information provided as part of the Material Inspection and Receiving Report specified elsewhere in this contract, the Contractor shall report at the time of delivery, as part of the Material Inspection and Receiving Report, the following information:

(1) Unique item identifier.

(2) Unique item identifier type.

(3) Issuing agency code (if concatenated unique item identifier is used).

(4) Enterprise identifier (if concatenated unique item identifier is used).



- (5) Original part number (if there is serialization within the original part number).
- (6) Lot or batch number (if there is serialization within the lot or batch number).
- (7) Current part number (optional and only if not the same as the original part number).
- (8) Current part number effective date (optional and only if current part number is used).
- (9) Serial number (if concatenated unique item identifier is used).
- (10) Government's unit acquisition cost.
- (11) Unit of measure.
- (12) Type designation of the item as specified in the contract schedule, if any.
- (13) Whether the item is an item of Special Tooling or Special Test Equipment.
- (14) Whether the item is covered by a warranty.

(e) For embedded subassemblies, components, and parts that require DoD item unique identification under paragraph (c)(1)(iii) of this clause or when item unique identification is provided under paragraph (c)(1)(v), the Contractor shall report as part of the Material Inspection and Receiving Report specified elsewhere in this contract, the following information:

- (1) Unique item identifier of the parent item under paragraph (c)(1) of this clause that contains the embedded subassembly, component, or part.
- (2) Unique item identifier of the embedded subassembly, component, or part.
- (3) Unique item identifier type.\*\*
- (4) Issuing agency code (if concatenated unique item identifier is used).\*\*
- (5) Enterprise identifier (if concatenated unique item identifier is used).\*\*
- (6) Original part number (if there is serialization within the original part number).\*\*
- (7) Lot or batch number (if there is serialization within the lot or batch number).\*\*
- (8) Current part number (optional and only if not the same as the original part number).\*\*
- (9) Current part number effective date (optional and only if current part number is used).\*\*
- (10) Serial number (if concatenated unique item identifier is used).\*\*
- (11) Description.

\*\* Once per item.

(f) The Contractor shall submit the information required by paragraphs (d) and (e) of this clause as follows:



(1) End items shall be reported using the receiving report capability in Wide Area WorkFlow (WAWF) in accordance with the clause at [252.232-7003](#). If WAWF is not required by this contract, and the contractor is not using WAWF, follow the procedures at <http://dodprocurementtoolbox.com/site/uidregistry/>.

(2) Embedded items shall be reported by one of the following methods—

(i) Use of the embedded items capability in WAWF;

(ii) Direct data submission to the IUID Registry following the procedures and formats at <http://dodprocurementtoolbox.com/site/uidregistry/>; or

(iii) Via WAWF as a deliverable attachment for exhibit line item number (fill in) \_\_\_\_, Unique Item Identifier Report for Embedded Items, Contract Data Requirements List, DD Form 1423.

(g) Subcontracts. If the Contractor acquires by subcontract any item(s) for which item unique identification is required in accordance with paragraph (c)(1) of this clause, the Contractor shall include this clause, including this paragraph (g), in the applicable subcontract(s), including subcontracts for commercial products or commercial services.

(End of clause)

252.225-7016 (Jan 2023) restriction on Acquisition of Ball and Roller Bearings:

(a) Definitions. As used in this clause—

(1) “Bearing components” means the bearing element, retainer, inner race, or outer race.

(2) “Component,” other than a bearing component, means any item supplied to the Government as part of an end product or of another component.

(3) “End product” means supplies delivered under a line item of this contract.

(b) Except as provided in paragraph (c) of this clause—

(1) Each ball and roller bearing delivered under this contract shall be manufactured in the United States, its outlying areas, or Canada; and

(2) For each ball or roller bearing, the cost of the bearing components manufactured in the United States, its outlying areas, or Canada shall exceed 50 percent of the total cost of the bearing components of that ball or roller bearing.

(c) The restriction in paragraph (b) of this clause does not apply to ball or roller bearings that are acquired as—

(1) Commercial components of an other than commercial; or

(2) Commercial or other than commercial components of an commercial component of a other than commercial end product.



(d) The restriction in paragraph (b) of this clause may be waived upon request from the Contractor in accordance with subsection [225.7009-4](#) of the Defense Federal Acquisition Regulation Supplement.

(e) If this contract includes DFARS clause [252.225-7009](#) , Restriction on Acquisition of Certain Articles Containing Specialty Metals, all bearings that contain specialty metals, as defined in that clause, must meet the requirements of that clause.

(f) Subcontracts. The Contractor shall insert the substance of this clause, including this paragraph (f), in all subcontracts, except those for—

(1) Commercial products; or

(2) Items that do not contain ball or roller bearings.

(End of clause)

252.244-7000 (Jan 2023) Subcontracts for Commercial Products or Commercial Services:

(a) The Contractor is not required to flow down the terms of any Defense Federal Acquisition Regulation Supplement (DFARS) clause in subcontracts for commercial products or commercial services at any tier under this contract, unless so specified in the particular clause.

(b) While not required, the Contractor may flow down to subcontracts for commercial products or commercial services a minimal number of additional clauses necessary to satisfy its contractual obligation.

(c)(1) In accordance with [10 U.S.C. 3457\(c\)](#) , the Contractor shall treat as commercial items any products valued at less than \$10,000 per item that were purchased by the Contractor for use in the performance of multiple contracts with the Department of Defense and other parties and are not identifiable to any particular contract when purchased.

(2) The Contractor shall ensure that any items to be used in performance of this contract, that are treated as commercial products pursuant to paragraph (c)(1) of this clause, meet all terms and conditions of this contract that are applicable to commercial products in accordance with the clause at Federal Acquisition Regulation 52.244-6 and paragraph (a) of this clause.

(d) The Contractor shall include the terms of this clause, including this paragraph (d), in subcontracts awarded under this contract, including subcontracts for the acquisition of commercial products or commercial services.

(End of clause)

252.204-7012(Dec 2019) Safeguarding Covered Defense Information and Cyber Incident Reporting:

(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—Other Than Commercial Products and Commercial Services, 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](mailto: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 products or commercial services, 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)

252.204-7015 (Jan 2023) Notice of Authorized Disclosure for Litigation Support:

(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) Subcontracts. Include the substance of this clause, including this paragraph (c), in all subcontracts, including subcontracts for commercial products or commercial services.

(End of clause)