

SPRPA1-12-D-001Y ORDER 5002

PART I - THE SCHEDULE
SECTION F
DELIVERIES OR PERFORMANCE

5252.225-9408

VERIFICATION OF "SHIP TO" AND/OR "NOTICE OF AVAILABILITY" ADDRESS (JAN 1992)

The contractor shall submit a request in duplicate to the Transportation Office of the cognizant Contract Administration Office for verification of the "Ship to" address. If the offer/release instructions require a "Notice of Availability" the contractor shall also request verification of the address to which notification will be made (the 'IAC3' address). Such requests shall be submitted at least ten (10) days in advance of (i) date "Notice of Availability" is to be submitted; or (ii) actual shipping date, if shipment is to be released automatically.

NAVSUPWSSFA03

TRANSPORTATION ASSISTANCE (MAY 2010)

To obtain transportation assistance for an upcoming shipment, contractors are to follow the appropriate directions listed below, based on the terms and conditions of the specific contract.

1. For all contracts administered by a Defense Contract Management Agency (DCMA) office (as shown on Page 1 of the contract, or in a subsequent modification), contractors are to contact the Transportation Office at that DCMA.

If the DCMA Transportation Office is unable to provide assistance, contractors may contact NAVSUP WSS Code 0344.03 at (215) 697-2715.

2. For Fast Payment FOB Origin contracts administered by the NAVSUP WSS Mechanicsburg contracting officer (as shown on Page 1 of the contract, or in a subsequent modification), the contractor must first electronically submit a Ready-to-Ship notice to the Naval Operational Logistics Support Center (NOLSC) through their website <https://www.navsupsup.navy.mil/site/rtts/>. Contractors with questions or problems may contact the NOLSC Shipment Processing Office via email address: nolsc_sts@navy.mil (preferred method). In an emergency, contractors may contact them at (757) 443-5449.

For this type of contract, additional information can be found in the clause NAVSUPWSSFA20 entitled "NOLSC-SP WEB-BASED CONTRACTOR SHIPMENT REQUEST PROCEDURES -- FOB ORIGIN FAST PAY."

3. For FOB Destination contracts, consignment address information is available electronically at the DoD Activity Address Codes (DODAAC) website: <https://www.daas.dla.mil/daasinq/dodaac.asp?cu=d>.

For this type of contract, additional information can be found in the clause NAVSUPWSSLA10 entitled "CONSIGNMENT INSTRUCTIONS."

NAVSUPWSSFA08

FMS DELIVERY AND SHIPPING INSTRUCTIONS (MAR 2004)

Material to be delivered FOB Origin at or near contractor's plant in the manner specified below. Use of Agency Official Indicia mail by contractors is not authorized. Quantities will not be divided into mailable lots for the express purpose of avoiding movement by other modes of transportation.

Consignment instructions provided herein are subject to change. In order to obtain the most current "Ship To" and "Mark For" information, the contractor is required to contact the cognizant DCMA Transportation Office ten days prior to shipment.

MATERIAL/TRANSPORTATION DATA:

If shipment qualifies as a small parcel under current specifications, ship via a Mode 5 small parcel carrier within the Continental United States (CONUS). Contractor will add prepaid transportation charges as a separate item on the invoice for reimbursement purposes.

If shipment does not qualify as a small parcel (Mode 5) shipment, ship to the Freight Forwarder on a collect commercial Bill of Lading.

International FMS Parcel Post (PP) shipments destined for the Government of Canada will be made via "Certificate of

SPRPA1-12-D-001Y ORDER 5002

NAVSUPWSSFA08 (CONT)
FMS DELIVERY AND SHIPPING INSTRUCTIONS (MAR 2004)

Mailing" using United States Postal Service (USPS) Form 3817, 3877 or 3877A.

If an X appears in the following parentheses (<X>), ship on a Prepaid Commercial Bill of Lading (CBL). Request transportation instructions from the cognizant DCMA Transportation Office. Transportation Account Code (TAC) <PSAE> applies.

SPECIAL MARKINGS:

For record accounting identification purposes, the Document Number, National Stock Number (NSN), and Supplementary Address, which appear under each line item(s) subclin, must be referenced in all Contracts, Invoices, Shipping, Inspection, and Financial Documents.

For FMS shipments only, regardless of size, the shipper shall bar code and apply the below listed identification with the appropriate bar coding format as specified in the MILSTD-129-P (disregarding 4.4.1.2) based on the packaging standard used.

The Bar Code Lines should read as shown below.

(NOTE: The 14-15 position Requisition Number, which can be found under each line item(s) subclin, shall be bar coded vice the Contract number.)

BAR CODE LINE 1:

National Stock Number (NSN) or CAGE and Part Number (if no NSN)

BAR CODE LINE 2:

Requisition Number(s) (be sure to include each Requisition Number in the multi -pack)

BAR CODE LINE 3:

Unit of Issue, Quantity, Unit Price, Supplementary Address

The information to be bar coded is reflected in the DD250 as follows:

Block 13	Supplementary Address (8 position alphanumeric code)
Block 16	National Stock Number (NSN) or CAGE/Part Number
Block 17	Quantity
Block 18	Unit(of Issue)
Block 19	Unit Price

DISTRIBUTION OF MATERIAL INSPECTION AND RECEIVING REPORTS (DD250)
AND BILLS OF LADING

- (1) Attach four (4) copies of DD250 in waterproof envelope outside of shipping container.
- (2) Forward two (2) copies of DD250 annotated by carrier as proof of shipment to NAVSUP WSS-PHIL, 700 Robbins Avenue, Philadelphia, PA 19111, Code 754, at the time of shipment.
- (3) Forward three (3) copies of DD250 to designated Freight Forwarder.
- (4) Where NAVSUP WSS-PHIL is the status control activity, forward two (2) copies of DD250 to the attention of

Thomas Kuhnle@DLA.mil

SPRPA1-12-D-001Y ORDER 5002

NAVSUPWSSFA08 (CONT)
 SMS DELIVERY AND SHIPPING INSTRUCTIONS (MAR 2004)

NAVSUP WSS-PHIL Code 0142. Where the status control activity is other than NAVSUP WSS-PHIL, forward one (1) copy of DD250 to NAVSUP WSS-PHIL Code 0142 and one (1) copy of DD250 to the status control activity.
 (5) Forward one (1) copy of DD250 to NAVSUP WSS-PHIL Code P75 <P7511.51> .

PART I - THE SCHEDULE
 SECTION G
 CONTRACT ADMINISTRATION DATA

ACRN			AMOUNT	TAC
AA	97-11X824228180007418200659182DPDEN54329560510SAE		\$8,378.98	

252.232-7008
 WIDE AREA WORKFLOW PAYMENT INSTRUCTIONS (MAY 2013)

(a) DEFINITIONS. As used in this clause-

"Department of Defense Activity Address Code (DoDAAC)" is a six position code that uniquely identifies a unit, activity, or organization.

"Document type" means the type of payment request or receiving report available for creation in Wide Area Work Flow (WAWF).

"Local processing office (LPO)" is the office responsible for payment certification when payment certification is done external to the entitlement system.

(b) ELECTRONIC INVOICING. The WAWF system is the method to electronically process vendor payment requests and receiving reports, as authorized by DFARS 252.232-7003, Electronic Submission of Payment Requests and Receiving Reports.

(c) WAWF ACCESS. To access WAWF, the Contractor shall-

- (1) Have a designated electronic business point of contact in the System for Award Management at <https://www.acquisition.gov>; and
- (2) Be registered to use WAWF at <https://wawf.eb.mil/> following the step-by-step procedures for self-registration available at this web site.

(d) WAWF TRAINING. The Contractor should follow the training instructions of the WAWF Web-Based Training Course and use the Practice Training Site before submitting payment requests through WAWF. Both can be accessed by selecting the "Web Based Training" link on the WAWF home page at <https://wawf.eb.mil/>

(e) Document submissions may be via web entry, Electronic Data Interchange, or File Transfer Protocol.

(f) WAWF PAYMENT INSTRUCTIONS. The Contractor must use the following information when submitting payment requests and receiving reports in WAWF for this contract/order:

- (1) DOCUMENT TYPE. The Contractor shall use the following document type(s).
 <INVOICE & RECEIVING REPORT (COMBO)> (Contracting Officer: Insert applicable document type(s).

NOTE: If a "Combo" document type is identified but not supportable by the Contractor's business systems, and Invoice (stand-alone) and "Receiving Report" (stand-alone) document type may be used instead.)

(2) INSPECTION/ACCEPTANCE LOCATION. The Contractor shall select the following inspection/acceptance location(s) in WAWF, as specified by the contracting officer.

<INSPECTION SITE: SOURCE, FINAL ACCEPTANCE: SOURCE> (Contracting Officer: Insert inspection and acceptance locations or "Not applicable.")

SPRPA1-12-D-001Y ORDER 5002

252.232-7008 (CONT)
WIDE AREA WORKFLOW PAYMENT INSTRUCTIONS (MAY 2013)

(3) DOCUMENT ROUTING. The Contractor shall use the information in the Routing Data Table below only to fill in applicable fields in WAWF when creating payment requests and receiving reports in the system.

ROUTING DATA TABLE*

FIELD NAME IN WAWF	DATA TO BE ENTERED IN WAWF
Pay Official DoDAAC:	<HQ0339>
Issue By DoDAAC:	<SPRPA1>
Admin DoDAAC:	<S4801A>
Inspect By DoDAAC:	<S4801A>
Ship To Code:	<SEE SCHEDULE>
Ship From Code:	<TBD>
Mark For Code:	<N/A>
Service Approver (DoDAAC):	<N/A>
Service Acceptor (DoDAAC):	<08748>
Accept at Other DoDAAC:	<N/A>
LPO DoDAAC:	<N65916>
DCAA Auditor DoDAAC:	<N/A>
Other DoDAAC(s):	<N/A>

(*Contracting Officer: Insert applicable DoDAAC information or "See schedule" if multiple ship to/acceptance locations apply, or "Not applicable.")

(4) PAYMENT REQUEST AND SUPPORTING DOCUMENTATION. The Contractor shall ensure a payment request includes appropriate contract line item and subline item descriptions of the work performed or supplies delivered, unit price/cost per unit, fee (if applicable), and all relevant back-up documentation, as defined in DFARS Appendix F, (e.g. timesheets) in support of each payment request.

(5) WAWF EMAIL NOTIFICATIONS. The Contractor shall enter the e-mail address identified below in the "Send Additional Email Notifications" field of WAWF once a document is submitted in the system.
 <N/A> (Contracting Officer: Insert applicable email addresses or "Not applicable.")

(g) WAWF POINT OF CONTACT.

(1) The Contractor may obtain clarification regarding invoicing in WAWF from the following contracting activity's WAWF point of contact.

Shirley Young, Code 0252.07, at 717-605-1134 or via shirley.young@navy.mil

(2) For technical WAWF help, contact the WAWF helpdesk at 866-618-5988.

NAVSUPWSSGA07
RECONSIGNMENT DIRECTIONS (MAR 2004)

authority is hereby delegated to the contract administration office to issue "No Cost" reconsignment directions to the contractor pursuant to requests made by the contracting activity.

NAVSUPWSSGA13
ONE NAVSUP" INITIATIVE - NAME CHANGE FROM NAVICP TO NAVSUP WEAPON SYSTEMS SUPPORT (NAVSUP WSS) (JUN 2011)

NOTE: This clause is not applicable to procurement documents issued by either of the following
 Defense Logistics Agency (DLA) Detachments:
 (SPRMM1) DLA Mechanicsburg (Maritime), 5450 Carlisle Pike, Mechanicsburg, PA 17055-0788
 (SPRPA1) DLA Philadelphia (Aviation), 700 Robbins Avenue, Philadelphia, PA 19111-5098

On 01 July 2011, a Naval Supply Systems Command (NAVSUP) initiative goes into effect changing the names of all activities within the NAVSUP Enterprise to provide a clear understanding of NAVSUP's mission in Navy's Global Logistics Support Network, and to present itself as a single, collaborative organization. Each activity will execute its mission as a node of this network. To comply with this initiative, the following name change will be effective on that date:

FROM:

SPRPA1-12-D-001Y ORDER 5002

NAVSUPWSSGA13 (CONT)
 ONE NAVSUP" INITIATIVE - NAME CHANGE FROM NAVICP TO NAVSUP WEAPON SYSTEMS SUPPORT (NAVSUP WSS) (JUN 2011)

(N00104) Naval Inventory Control Point (NAVICP) Mechanicsburg
 5450 Carlisle Pike
 Mechanicsburg, PA 17055-0788

(N00383) Naval Inventory Control Point (NAVICP) Philadelphia
 700 Robbins Avenue
 Philadelphia, PA 19111-5098

TO:
 (N00104) NAVSUP Weapon Systems Support (NAVSUP WSS), Mechanicsburg Site
 5450 Carlisle Pike
 Mechanicsburg, PA 17055-0788

(N00383) NAVSUP Weapon Systems Support (NAVSUP WSS), Philadelphia Site
 700 Robbins Avenue
 Philadelphia, PA 19111-5098

New contract awards and modifications issued on and after 01 July 2011 will contain the new activity name NAVSUP Weapon Systems Support (NAVSUP WSS). Existing contracts issued prior to 01 July 2011 will contain the old activity name Naval Inventory Control Point (NAVICP), and will only be modified to change the activity name as part of a future contract modification issued for an unrelated reason.

PART II - CONTRACT CLAUSES
 SECTION I
 CONTRACT CLAUSES

252.225-7002
 QUALIFYING COUNTRY SOURCES AS SUBCONTRACTORS (DEC 2012)

252.225-7021
 TRADE AGREEMENTS (DEC 2012)

252.225-7001
 RESTRICTION OF ACQUISITION OF SUPERCOMPUTERS (JUNE 2005)

Supercomputers delivered under this contract shall be manufactured in the United States or its outlying areas.

252.225-7038
 BUY AMERICAN ACT--FREE TRADE AGREEMENTS-BALANCE OF PAYMENTS PROGRAM (DEC 2010)

The basic clause at 252.225-7038 applies when the estimated value equals or exceeds \$70,079.
 The clause with its Alternate I (JUL 2009) applies when the estimated value equals or exceeds \$25,000 but is less than \$70,079.

252.232-7003
 ELECTRONIC SUBMISSION OF PAYMENT REQUESTS AND RECEIVING REPORTS (JUN 2012)

252.225-7012
 REFERENCE FOR CERTAIN DOMESTIC COMMODITIES (DEC 2012)

2.219-28
 POST-AWARD SMALL BUSINESS PROGRAM REREPRESENTATION (JUL 2013)

(a) Definitions. As used in this clause-
 Long-term contract" means a contract of more than five years in duration, including options. However, the term does not include contracts that exceed five years in duration because the period of performance has been extended for a cumulative period not to exceed six months under the clause at 2.217-8, Option to Extend Services, or other appropriate authority.

SPRPA1-12-D-001Y ORDER 5002

52.219-28 (CONT)
POST-AWARD SMALL BUSINESS PROGRAM REREPRESENTATION (JUL 2013)

"Small business concern" means a concern, including its affiliates, that is independently owned and operated, not dominant in the field of operation in which it is bidding on Government contracts, and qualified as a small business under the criteria in 13 CFR part 121 and the size standard in paragraph (c) of this clause. Such a concern is "not dominant in its field of operation" when it does not exercise a controlling or major influence on a national basis in a kind of business activity in which a number of business concerns are primarily engaged. In determining whether dominance exists, consideration shall be given to all appropriate factors, including volume of business, number of employees, financial resources, competitive status or position, ownership or control of materials, processes, patents, license agreements, facilities, sales territory, and nature of business activity.

(b) If the Contractor represented that it was a small business concern prior to award of this contract, the Contractor shall rerepresent its size status according to paragraph (e) of this clause or, if applicable, paragraph (g) of this clause, upon the occurrence of any of the following:

- (1) Within 30 days after execution of a novation agreement or within 30 days after modification of the contract to include this clause, if the novation agreement was executed prior to inclusion of this clause in the contract.
- (2) Within 30 days after a merger or acquisition that does not require a novation or within 30 days after modification of the contract to include this clause, if the merger or acquisition occurred prior to inclusion of this clause in the contract.
- (3) For long-term contracts-
 - (i) Within 60 to 120 days prior to the end of the fifth year of the contract; and
 - (ii) Within 60 to 120 days prior to the date specified in the contract for exercising any option thereafter.

(c) The Contractor shall rerepresent its size status in accordance with the size standard in effect at the time of this rerepresentation that corresponds to the North American Industry Classification System (NAICS) code assigned to this contract. The small business size standard corresponding to this NAICS code can be found at: <http://www.sba.gov/content/table-small-business-size-standards>.

(d) The small business size standard for a Contractor providing a product which it does not manufacture itself, for a contract other than a construction or service contract, is 500 employees

(e) Except as provided in paragraph (g) of this clause, the Contractor shall make the representation required by paragraph (b) of this clause by validating or updating all its representations in the Representations and Certifications section of the System for Award Management (SAM) and its other data in SAM, as necessary, to ensure that they reflect the Contractor's current status. The Contractor shall notify the contracting office in writing within the timeframe specified in paragraph (b) of this clause, that the data have been validated or updated, and provide the date of the validation or update.

(f) If the Contractor represented that it was other than a small business concern prior to award of this contract, the Contractor may, but is not required to, take the actions required by paragraphs (e) or (g) of this clause.

(g) If the Contractor does not have representations and certifications in SAM, or does not have a representation in SAM for the NAICS code applicable to this contract, the Contractor is required to complete the following rerepresentation and submit it to the contracting office, along with the contract number and the date on which the rerepresentation was completed:

The Contractor represents that it () is, () is not a small business concern under NAICS Code _____ assigned to contract number _____. (Contractor to sign and date and insert authorized signer's name and title)

52.203-7000
REQUIREMENTS RELATING TO COMPENSATION OF FORMER DOD OFFICIALS (SEP 2011)

- (a) Definition. "Covered DoD official," as used in this clause, means an individual that-
- (1) Leaves or left DoD service on or after January 28, 2008; and
 - (2)(i) Participated personally and substantially in an acquisition as defined in 41 U.S.C. 131 with a value in excess of \$10 million, and serves or served-
 - (A) In an Executive Schedule position under subchapter II of chapter 53 of Title 5, United States

SPRPA1-12-D-001Y ORDER 5002

252.203-7000 (CONT)
REQUIREMENTS RELATING TO COMPENSATION OF FORMER DOD OFFICIALS (SEP 2011)

Code;

(B) In a position in the Senior Executive Service under subchapter VIII of chapter 53 of Title 5, United States Code; or

(C) In a general or flag officer position compensated at a rate of pay for grade O-7 or above under section 201 of Title 37, United States Code; or

(ii) Serves or served in DoD in one of the following positions: program manager, deputy program manager, procuring contracting officer, administrative contracting officer, source selection authority, member of the source selection evaluation board, or chief of a financial or technical evaluation team for a contract in an amount in excess of \$10 million.

(b) The Contractor shall not knowingly provide compensation to a covered DoD official within 2 years after the official leaves DoD service, without first determining that the official has sought and received, or has not received after 30 days of seeking, a written opinion from the appropriate DoD ethics counselor regarding the applicability of post-employment restrictions to the activities that the official is expected to undertake on behalf of the Contractor.

(c) Failure by the Contractor to comply with paragraph (b) of this clause may subject the Contractor to rescission of this contract, suspension, or debarment in accordance with 41 U.S.C. 2105(c).

252.225.7015
RESTRICTION ON ACQUISITION OF HAND OR MEASURING TOOLS (JUNE 2005)

252.225-7028
EXCLUSIONARY POLICIES AND PRACTICES OF FOREIGN GOVERNMENTS (APR 2003)

252.204-7012
SAFEGUARDING OF UNCLASSIFIED CONTROLLED TECHNICAL INFORMATION (NOV 2013)

(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.

"Attribution information" means information that identifies the Contractor, whether directly or indirectly, by the grouping of information that can be traced back to the Contractor (e.g., program description or facility locations).

"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 information system" means an information system belonging to, or operated by or for, the Contractor.

"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 is to be marked with one of the distribution statements B-through-F, in accordance with DoD Instruction 5230.24, Distribution Statements on Technical Documents. The term does not include information that is lawfully publicly available without restrictions.

"Cyber incident" means actions taken through the use of computer networks that result in an actual or potentially diverse effect on an information system and/or the information residing therein.

"Exfiltration" means any unauthorized release of data from within an information system. This includes copying the data through covert network channels or the copying of data to unauthorized media.

"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 information is recorded, stored, or

SPRPA1-12-D-001Y ORDER 5002

252.204-7012 (CONT)
SAFEGUARDING OF UNCLASSIFIED CONTROLLED TECHNICAL INFORMATION (NOV 2013)

printed within an 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-Non Commercial 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) Safeguarding requirements and procedures for unclassified controlled technical information. The Contractor shall provide adequate security to safeguard unclassified controlled technical information from compromise. To provide adequate security, the Contractor shall--

(1) Implement information systems security in its project, enterprise, or company-wide unclassified information technology system(s) that may have unclassified controlled technical information resident on or transiting through them. The information systems security program shall implement, at a minimum--

(i) The specified National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 security controls identified in the following table; or

(ii) If a NIST control is not implemented, the Contractor shall submit to the Contracting Officer a written explanation of how--

(A) The required security control identified in the following table is not applicable; or

(B) An alternative control or protective measure is used to achieve equivalent protection.

(2) Apply other information systems security requirements when the Contractor reasonably determines that information systems security measures, in addition to those identified in paragraph (b)(1) of this clause, may be required to provide adequate security in a dynamic environment based on an assessed risk or vulnerability.

Table 1 -- Minimum Security Controls for Safeguarding

Minimum required security controls for unclassified controlled technical information requiring safeguarding in accordance with paragraph (d) of this clause. (A description of the security controls is in the NIST SP 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations" (<http://csrc.nist.gov/publications/PubsSPs.html>)).

Access Control	Audit & Accountability	Identification and Authentication	Media Protection	System & Comm Protection
AC-2	AU-2	IA-2	MP-4	SC-2
AC-3(4)	AU-3	IA-2	MP-6	SC-2
AC-4	AU-6(1)	IA-4		SC-4
AC-6	AU-7	IA-5(1)	Physical and Environmental Protection	SC-7
AC-7	AU-8			SC-8(1)
AC-11(1)	AU-9	Incident Response	PE-2	SC-13
AC-17(2)		IR-2	PE-3	SC-15
AC-18(1)		IR-4	PE-5	SC-28
AC-19	Configuration Management	IR-5	Program Management	
AC-20(1)	CM-2	IR-6		
AC-20(2)	CM-6			
AC-22	CM-7			
	CM-8			
		Maintenance		System & Information Integrity
		MA-4(6)		SI-2
Awareness & Training	Contingency Planning	MA-5	Risk Assessment	SI-3
AT-2	CP-9	MA-6	RA-5	SI-4

Legend:

AC: Access Control	MA: Maintenance
AT: Awareness and Training	MP: Media Protection
AU: Auditing and Accountability	PE: Physical & Environmental Protection
CM: Configuration Management	PM: Program Management
CP: Contingency Planning	RA: Risk Assessment
IA: Identification and Authentication	SC: System & Communications Protection
IR: Incident Response	SI: System & Information Integrity

SPRPA1-12-D-001Y ORDER 5002

252.204-7012 (CONT)

SAFEGUARDING OF UNCLASSIFIED CONTROLLED TECHNICAL INFORMATION (NOV 2013)

(c) Other requirements. This clause does not relieve the Contractor of the requirements specified by applicable statutes or other Federal and DoD safeguarding requirements for Controlled Unclassified Information (CUI) as established by Executive Order 13556, as well as regulations and guidance established pursuant thereto.

(d) Cyber incident and compromise reporting.

(1) Reporting requirement. The Contractor shall report as much of the following information as can be obtained to the Department of Defense via (<http://dibnet.dod.mil/>) within 72 hours of discovery of any cyber incident, as described in paragraph (d)(2) of this clause, that affects unclassified controlled technical information resident on or transiting through the Contractor's unclassified information systems:

- (i) Data Universal Numbering System (DUNS)
- (ii) Contract numbers affected unless all contracts by the company are affected.
- (iii) Facility CAGE code if the location of the event is different than the prime Contractor location.
- (iv) Point of contact if different than the POC recorded in the System for Award Management (address, position, telephone, email).
- (v) Contracting Officer point of contact (address, position, telephone, email).
- (vi) Contract clearance level.
- (vii) Name of subcontractor and CAGE code if this was an incident on a Sub-contractor network.
- (viii) DoD programs, platforms or systems involved.
- (ix) Location(s) of compromise.
- (x) Date incident discovered.
- (xi) Type of compromise (e.g., unauthorized access, inadvertent release, other).
- (xii) Description of technical information compromised.
- (xiii) Any additional information relevant to the information compromise.

(2) Reportable cyber incidents. Reportable cyber incidents include the following:

(i) A cyber incident involving possible exfiltration, manipulation, or other loss or compromise of any unclassified controlled technical information resident on or transiting through Contractor's, or its subcontractors', unclassified information systems.

(ii) Any other activities not included in paragraph (d)(2)(i) of this clause that allow unauthorized access to the Contractor's unclassified information system on which unclassified controlled technical information is resident on or transiting.

(3) Other reporting requirements. This reporting in no way abrogates the Contractor's responsibility for additional safeguarding and cyber incident reporting requirements pertaining to its unclassified information systems under other clauses that may apply to its contract, or as a result of other U.S. Government legislative and regulatory requirements that may apply (e.g., as cited in paragraph (c) of this clause).

(4) Contractor actions to support DoD damage assessment. In response to the reported cyber incident, the Contractor shall-

(i) Conduct further review of its unclassified network for evidence of compromise resulting from a cyber incident to include, but is not limited to, identifying compromised computers, servers, specific data and users accounts. This includes analyzing information systems that were part of the compromise, as well as other information systems on the network that were accessed as a result of the compromise;

(ii) Review the data accessed during the cyber incident to identify specific unclassified controlled technical information associated with DoD programs, systems or contracts, including military programs, systems and technology; and

(iii) Preserve and protect images of known affected information systems and all relevant monitoring/packet capture data for at least 90 days from the cyber incident to allow DoD to request information or decline interest.

(5) DoD damage assessment activities. If DoD elects to conduct a damage assessment, the Contracting Officer will request that the Contractor point of contact identified in the incident report at (d)(1) of this clause provide all of the damage assessment information gathered in accordance with paragraph (d)(4) of this clause. The Contractor shall comply with damage assessment information requests. The requirement to share files and images exists unless there are legal restrictions that limit a company's ability to share digital media. The Contractor shall inform the Contracting Officer of the source, nature, and prescription of such limitations and the authority responsible.

(e) Protection of reported information. Except to the extent that such information is lawfully publicly available without restrictions, the Government will protect information reported or otherwise provided to DoD under this clause in accordance with applicable statutes, regulations, and policies. The Contractor shall identify and mark attribution information reported or otherwise provided to the DoD. The Government may use information, including attribution information and disclose it only to authorized persons for purposes and activities consistent with this clause.

(f) Nothing in this clause limits the Government's ability to conduct law enforcement or counterintelligence activities, or other lawful activities in the interest of homeland security and national security. The results of the activities described in this clause may be used to support an investigation and prosecution of any person or entity, including those attempting to infiltrate or compromise information on a contractor information system in violation of any statute.

SPRPA1-12-D-001Y ORDER 5002

252.204-7012 (CONT)
SAFEGUARDING OF UNCLASSIFIED CONTROLLED TECHNICAL INFORMATION (NOV 2013)

(g) Subcontracts. The Contractor shall include the substance of this clause, including this paragraph (g), in all subcontracts, including subcontracts for commercial items.

52.222-29
NOTIFICATION OF VISA DENIAL (JUNE 2003)

52.223-18
ENCOURAGING CONTRACTOR POLICIES TO BAN TEXT MESSAGING WHILE DRIVING (AUG 2011)

52.211-15
DEFENSE PRIORITY AND ALLOCATION REQUIREMENTS (APRIL 2008)

52.209-6
PROTECTING THE GOVERNMENT'S INTEREST WHEN SUBCONTRACTING WITH CONTRACTORS DEBARRED, SUSPENDED, OR PROPOSED FOR DEBARMENT (AUG 2013)

52.209-10
PROHIBITION ON CONTRACTING WITH INVERTED DOMESTIC CORPORATIONS (MAY 2012)

52.232-23
ASSIGNMENT OF CLAIMS (JAN 1986)

52.222-19
CHILD LABOR-COOPERATION WITH AUTHORITIES AND REMEDIES (JAN 2014)

52.204-9
PERSONAL IDENTITY VERIFICATION OF CONTRACTOR PERSONNEL (JAN 2011)

52.204-2
SECURITY REQUIREMENTS (AUG 1996)

52.232-40
PROVIDING ACCELERATED PAYMENTS TO SMALL BUSINESS SUBCONTRACTORS (DEC 2013)

PART IV - REPRESENTATIONS AND INSTRUCTIONS
SECTION K
REPRESENTATIONS, CERTIFICATIONS, AND OTHER STATEMENTS OF OFFERORS OR QUOTERS

52.203-7005
REPRESENTATION RELATING TO COMPENSATION OF FORMER DOD OFFICIALS (NOV 2011)

(a) Definition. "Covered DoD official" is defined in the clause at 252.203-7000, Requirements Relating to Compensation of Former DoD Officials.

(b) By submission of this offer, the offeror represents, to the best of its knowledge and belief, that all covered DoD officials employed by or otherwise receiving compensation from the offeror, and who are expected to undertake activities on behalf of the offeror for any resulting contract, are presently in compliance with all post-employment restrictions covered by 18 U.S.C. 207, 41 U.S.C. 2101-2107, and 5 CFR parts 2637 and 2641, including Federal Acquisition Regulation 3.104-2.

52.225-7000
BUY AMERICAN STATUTE-BALANCE OF PAYMENTS PROGRAM-CERTIFICATE (JUN 2012)

(a) Definitions. "Commercially available off-the-shelf (COTS) item," "domestic end product," "component,"

SPRPA1-12-D-001Y ORDER 5002

252.225-7000 (CONT)

BUY AMERICAN STATUTE-BALANCE OF PAYMENTS PROGRAM-CERTIFICATE (JUN 2012)

"domestic end product" "foreign end product," "qualifying country," "qualifying country end product," and "United States" have the meanings given in the Buy American Act and Balance of Payments Program clause of this solicitation.

(b) Evaluation. The Government -

(1) Will evaluate offers in accordance with the policies and procedures of Part 225 of the Defense Federal Acquisition Regulation Supplement; and

(2) Will evaluate offers of qualifying country end products without regard to the restrictions of the Buy American Statute or the Balance of Payments Program.

(c) Certifications and identification of country of origin.

(1) For all line items subject to the Buy American and Balance of Payments Program clause of this solicitation, the offeror certifies that -

(i) Each end product, except those listed in paragraphs (c)(2) or (3) of this provision, is a domestic end product; and

(ii) For end products other than COTS items, components of unknown origin are considered to have been mined, produced, or manufactured outside the United States or a qualifying country.

(2) The offeror certifies that the following end products are qualifying country end products:

Line Item Number	Country of Origin
_____	_____
_____	_____
_____	_____
_____	_____

(3) The following end products are other foreign end products, including end products manufactured in the United States that do not qualify as domestic end products, i.e., and end product that is not a COTS item and does not meet the component test in paragraph (ii) of the definition of "domestic end product":

Line Item Number	Country of Origin (If Known)
_____	_____
_____	_____
_____	_____
_____	_____

PART IV - REPRESENTATIONS AND INSTRUCTIONS

SECTION L

INSTRUCTIONS, CONDITIONS, AND NOTICES TO OFFERORS OR QUOTERS

5252.204-9400

CONTRACTOR UNCLASSIFIED ACCESS TO FEDERALLY CONTROLLED FACILITIES, SENSITIVE INFORMATION, INFORMATION TECHNOLOGY (IT) SYSTEMS OR PROTECTED HEALTH INFORMATION (JULY 2013)

Homeland Security Presidential Directive (HSPD)-12, requires government agencies to develop and implement Federal

SPRPA1-12-D-001Y ORDER 5002

5252.204-9400 (CONT)

CONTRACTOR UNCLASSIFIED ACCESS TO FEDERALLY CONTROLLED FACILITIES, SENSITIVE INFORMATION, INFORMATION TECHNOLOGY (IT) SYSTEMS OR PROTECTED HEALTH INFORMATION (JULY 2013)

security standards for Federal employees and contractors. The Deputy Secretary of Defense Directive-Type Memorandum (DTM) 08-006 - "DoD Implementation of Homeland Security Presidential Directive - 12 (HSPD-12)" dated November 26, 2008 (or its subsequent DoD instruction) directs implementation of HSPD-12. This clause is in accordance with HSPD-12 and its implementing directives.

APPLICABILITY

This clause applies to contractor employees requiring physical access to any area of a federally controlled base, facility or activity and/or requiring access to a DoN or DoD computer/network/system to perform certain unclassified sensitive duties. This clause also applies to contractor employees who access Privacy Act and Protected Health Information, provide support associated with fiduciary duties, or perform duties that have been identified by DoN as National Security Position, as advised by the command security manager. It is the responsibility of the responsible security officer of the command/facility where the work is performed to ensure compliance.

Each contractor employee providing services at a Navy Command under this contract is required to obtain a Department of Defense Common Access Card (DoD CAC). Additionally, depending on the level of computer/network access, the contract employee will require a successful investigation as detailed below.

ACCESS TO FEDERAL FACILITIES

Per HSPD-12 and implementing guidance, all contractor employees working at a federally controlled base, facility or activity under this clause will require a DoD CAC. When access to a base, facility or activity is required contractor employees shall in-process with the Navy Command's Security Manager upon arrival to the Navy Command and shall out-process prior to their departure at the completion of the individual's performance under the contract. ACCESS TO DOD IT SYSTEMS In accordance with SECNAV M-5510.30, contractor employees who require access to DoN or DoD networks are categorized as IT-I, IT-II, or IT-III. The IT-II level, defined in detail in SECNAV M-5510.30, includes positions which require access to information protected under the Privacy Act, to include Protected Health Information (PHI). All contractor employees under this contract who require access to Privacy Act protected information are therefore categorized no lower than IT-II. IT Levels are determined by the requiring activity's Command Information Assurance Manager. Contractor employees requiring privileged or IT-I level access, (when specified by the terms of the contract) require a Single Scope Background Investigation (SSBI) which is a higher level investigation than the National Agency Check with Law and Credit (NACLC) described below. Due to the privileged system access, a SSBI suitable for High Risk public trust positions is required. Individuals who have access to system control, monitoring, or administration functions (e.g. system administrator, database administrator) require training and certification to Information Assurance Technical Level 1, and must be trained and certified on the Operating System or Computing Environment they are required to maintain.

Access to sensitive IT systems is contingent upon a favorably adjudicated background investigation. When access to IT systems is required for performance of the contractor employee's duties, such employees shall in-process with the Navy Command's Security Manager and Information Assurance Manager upon arrival to the Navy command and shall out-process prior to their departure at the completion of the individual's performance under the contract. Completion and approval of a System Authorization Access Request Navy (SAAR-N) form is required for all individuals accessing Navy Information Technology resources. The decision to authorize access to a government IT system/network is inherently governmental. The contractor supervisor is not authorized to sign the SAAR-N; therefore, the government employee with knowledge of the system/network access required or the COR shall sign the SAAR-N as the "supervisor".

The SAAR-N shall be forwarded to the Navy Command's Security Manager at least 30 days prior to the individual's start date. Failure to provide the required documentation at least 30 days prior to the individual's start date may result in delaying the individual's start date.

When required to maintain access to required IT systems or networks, the contractor shall ensure that all employees requiring access complete annual Information Assurance (IA) training, and maintain a current requisite background investigation. The Contractor's Security Representative shall contact the Command Security Manager for guidance when reinvestigations are required.

INTERIM ACCESS

The Navy Command's Security Manager may authorize issuance of a DoD CAC and interim access to a DoN or DoD unclassified computer/network upon a favorable review of the investigative questionnaire and advance favorable fingerprint results. When the results of the investigation are received and a favorable determination is not made, the contractor employee working on the contract under interim access will be denied access to the computer network and this denial will not relieve the contractor of his/her responsibility to perform.

SPRPA1-12-D-001Y ORDER 5002

5252.204-9400 (CONT)

CONTRACTOR UNCLASSIFIED ACCESS TO FEDERALLY CONTROLLED FACILITIES, SENSITIVE INFORMATION, INFORMATION TECHNOLOGY (IT) SYSTEMS OR PROTECTED HEALTH INFORMATION (JULY 2013)

DENIAL OR TERMINATION OF ACCESS

The potential consequences of any requirement under this clause including denial or termination of physical or system access in no way relieves the contractor from the requirement to execute performance under the contract within the timeframes specified in the contract. Contractors shall plan ahead in processing their employees and subcontractor employees. The contractor shall insert this clause in all subcontracts when the subcontractor is permitted to have unclassified access to a federally controlled facility, federally-controlled information system/network and/or to government information, meaning information not authorized for public release.

CONTRACTOR'S SECURITY REPRESENTATIVE

The contractor shall designate an employee to serve as the Contractor's Security Representative. Within three work days after contract award, the contractor shall provide to the requiring activity's Security Manager and the Contracting Officer, in writing, the name, title, address and phone number for the Contractor's Security Representative. The Contractor's Security Representative shall be the primary point of contact on any security matter. The Contractor's Security Representative shall not be replaced or removed without prior notice to the Contracting Officer and Command Security Manager.

BACKGROUND INVESTIGATION REQUIREMENTS AND SECURITY APPROVAL PROCESS FOR CONTRACTORS ASSIGNED TO NATIONAL SECURITY POSITIONS OR PERFORMING SENSITIVE DUTIES

Navy security policy requires that all positions be given a sensitivity value based on level of risk factors to ensure appropriate protective measures are applied. Navy recognizes contractor employees under this contract as Non-Critical Sensitive ADP/IT-II when the contract scope of work requires physical access to a federally controlled base, facility or activity and/or requiring access to a DoD computer/network, to perform unclassified sensitive duties. This designation is also applied to contractor employees who access Privacy Act and Protected Health Information (PHI), provide support associated with fiduciary duties, or perform duties that have been identified by DON as National Security Positions. At a minimum, each contractor employee must be a US citizen and have a favorably completed NACLIC to obtain a favorable determination for assignment to a non-critical sensitive or IT-II position. The NACLIC consists of a standard NAC and a FBI fingerprint check plus law enforcement checks and credit check. Each contractor employee filling a non-critical sensitive or IT-II position is required to complete:

- SF-86 Questionnaire for National Security Positions (or equivalent OPM investigative product)
- Two FD-258 Applicant Fingerprint Cards (or an electronic fingerprint submission)
- Original Signed Release Statements

Failure to provide the required documentation at least 30 days prior to the individual's start date shall result in delaying the individual's start date. Background investigations shall be reinitiated as required to ensure investigations remain current (not older than 10 years) throughout the contract performance period. The Contractor's Security Representative shall contact the Command Security Manager for guidance when reinvestigations are required.

Regardless of their duties or IT access requirements ALL contractor employees shall in-process with the Navy Command's Security Manager upon arrival to the Navy command and shall out process prior to their departure at the completion of individual's performance under the contract. Employees requiring IT access shall also check-in and check-out with the Navy Command's Information Assurance Manager. Completion and approval of a System Authorization Access Request Navy (SAAR-N) form is required for all individuals accessing Navy Information Technology resources. The SAAR-N shall be forwarded to the Navy Command's Security Manager at least 30 days prior to the individual's start date. Failure to provide the required documentation at least 30 days prior to the individual's start date shall result in delaying the individual's start date. The contractor shall ensure that each contract employee requiring access to IT systems or networks complete annual Information Assurance (IA) training, and maintain a current requisite background investigation. Contractor employees shall accurately complete the required investigative forms prior to submission to the Navy Command Security Manager. The Navy Command's Security Manager will review the submitted documentation for completeness prior to submitting it to the Office of Personnel Management (OPM). Suitability/security issues identified by the Navy may render the contractor employee ineligible for the assignment. An unfavorable determination made by the Navy is final (subject to SF-86 appeal procedures) and such a determination does not relieve the contractor from meeting any contractual obligation under the contract. The Navy Command's Security Manager will forward the required forms to OPM for processing. Once the investigation is complete, the results will be forwarded by OPM to the DON Central Adjudication Facility (CAF) for a determination.

If the contractor employee already possesses a current favorably adjudicated investigation, the contractor shall submit a Visit Authorization Request (VAR) via the Joint Personnel Adjudication System (JPAS) or a hard copy VAR directly from the contractor's Security Representative. Although the contractor will take JPAS "Owning" role over the contractor employee, the Navy Command will take JPAS "Servicing" role over the contractor employee during the

SPRPA1-12-D-001Y ORDER 5002

5252.204-9400 (CONT)

CONTRACTOR UNCLASSIFIED ACCESS TO FEDERALLY CONTROLLED FACILITIES, SENSITIVE INFORMATION, INFORMATION TECHNOLOGY (IT) SYSTEMS OR PROTECTED HEALTH INFORMATION (JULY 2013)

hiring process and for the duration of assignment under that contract. The contractor shall include the IT Position Category per SECNAV M-5510.30 for each employee designated on a VAR. The VAR requires annual renewal for the duration of the employee's performance under the contract.

BACKGROUND INVESTIGATION REQUIREMENTS AND SECURITY APPROVAL PROCESS FOR CONTRACTORS ASSIGNED TO OR PERFORMING NON-SENSITIVE DUTIES Contractor employee whose work is unclassified and non-sensitive (e.g., performing certain duties such as lawn maintenance, vendor services, etc ...) and who require physical access to publicly accessible areas to perform those duties shall meet the following minimum requirements:

- Must be either a US citizen or a US permanent resident with a minimum of 3 years legal residency in the United States (as required by The Deputy Secretary of Defense DTM 08-006 or its subsequent DoD instruction) and
- Must have a favorably completed National Agency Check with Written Inquiries (NACI) including a FBI fingerprint check prior to installation access.

To be considered for a favorable trustworthiness determination, the Contractor's Security Representative must submit for all employees each of the following:

- SF-85 Questionnaire for Non-Sensitive Positions
- Two FD-258 Applicant Fingerprint Cards (or an electronic fingerprint submission)
- Original Signed Release Statements

The contractor shall ensure each individual employee has a current favorably completed National Agency Check with Written Inquiries (NACI) or ensure successful FBI fingerprint results have been gained and investigation has been processed with OPM.

Failure to provide the required documentation at least 30 days prior to the individual's start date may result in delaying the individual's start date.

* Consult with your Command Security Manager and Information Assurance Manager for local policy when IT-III (non-sensitive) access is required for non-US citizens outside the United States.

252.225-7027**RESTRICTION ON CONTINGENT FEES FOR FOREIGN MILITARY SALES (APR 2003)**

(a) Except as provided in paragraph (b) of this clause, contingent fees, as defined in the Covenant Against Contingent Fees clause of this contract, are generally an allowable cost, provided the fees are paid to -

- (1) A bona fide employee of the Contractor, or
- (2) A bona fide established commercial or selling agency maintained by the Contractor for the purpose of securing business.

(b) For foreign military sales, unless the contingent fees have been identified and payment approved in writing by the foreign customer before contract award, the following contingent fees are unallowable under this contract:

- (1) For sales to the Government(s) of Australia, Taiwan, Egypt, Greece, Israel, Japan, Jordan, Republic of Korea, Kuwait, Pakistan, Philippines, Saudi Arabia, Turkey, Thailand, or Venezuela (Air Force) contingent fees in any amount.

- (2) For sales to Governments not listed in paragraph (b)(1) of this clause, contingent fees exceeding \$50,000 per foreign military sale case.

252.204-7011**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.

SPRPA1-12-D-001Y ORDER 5002

252.204-7011 (CONT)

ALTERNATIVE LINE ITEM STRUCTURE (SEP 2011)

(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 (DFARS/PGI view). 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		

252.246-7003

NOTIFICATION OF POTENTIAL SAFETY ISSUES (JUN 2013)

252.211-14

NOTICE OF PRIORITY RATING FOR NATIONAL DEFENSE, EMERGENCY PREPAREDNESS, AND ENERGY PROGRAM USE (APR 2008)

Any contract awarded as a result of this solicitation will be (< >) DX rated order; (< X >) DO rated order certified for national defense, emergency preparedness, and and energy program use under the Defense Priorities and Allocations System (DPAS) (15 CFR 700), and the Contractor will be required to follow all of the requirements of this regulation. (Contracting Officer check appropriate box).

NAVSUPWSSLA19

CONSIGNMENT INSTRUCTIONS (MAY 2010)

Consignment Addresses are readily available electronically at the DoD Activity Address Codes (DODAAC) website <https://www.daas.dla.mil/daasingq/dodaac.asp?cu=d>

Contractors are to enter a specific DODAAC Code (i.e. N03126), then select "Scan Query."

Three addresses will appear:

TAC1=Mailing Address TAC2=Shipping Address TAC3=Billing Address

The TAC2 Shipping Address should always be used.

If it is missing for whatever reason, the contractor is authorized to use the TAC1 Mailing Address.

For Mobile Units and Ships, call the Naval Operational Logistics Support Center (NOLSC) Fleet Locator at: Commercial 57-443-5434 or DSN 846-5434

SPRPA1-12-D-001Y ORDER 5002

CONSIGNMENT INSTRUCTIONS

NOTE: The activity codes listed below are used to identify the Activities which are to receive material. The activity code and the quantities to be shipped to each activity under this contract appear in the Schedule. DO NOT SHIP TO A WATER PORT OR AIR TERMINAL WITHOUT COMPLYING WITH THE CLEARANCE/MILSTAMP REQUIREMENTS OF CLAUSE FAR 52.247-52.

PDE005 Receiving Officer,

SPRPA1-12-D-001Y ORDER 5002

DISTRIBUTION

EXTERNAL:

(S4801A)
(E) DCMA SEATTLE

1 (N85916)
NAVSUP WSS PHIL FMS (MPN)

(HQ0339)
(E) DFAS - COLUMBUS CENTER

1 (08748)
(P) ELDEC CORPORATION

INTERNAL:

1 APAB.14

1 P754

1 P7611.51

1 FILE COPY