Product Delivery Order Requirements Package Checklist

Instructions: Use the below checklist to complete your delivery order package. Once complete, submit it to your Contracting Officer (CO) via AFWay with the applicable documents defined below. Please use the AFWay Customer Ordering Instructions for Products at Appendix P9 if you have questions. If you are using a GPC for the procurement of products, please use this checklist to ensure that all applicable acquisition and IT standards are met.
Note: Asterisked (*) items are mandatory for use in the acquisition of NetCentric Products

	DOCUMENTATION	REFERENCE	Check if Complete. Answer Yes/No/N/A Where Appropriate
1. DELIVERY ORDER INFORMATION			
a.	*Agency or Department: *Organization Office Symbol: *Organization Address:		☐ Yes ☐ No
b.	*DO Title: *Brief Description:		☐ Yes ☐ No
c.	*Primary POC from Requiring Activity: Name: Title: Email: Phone: Alternate POC for Requiring Activity: Name: Title: Email: Phone:		☐ Yes ☐ No
2. MARKET RESEARCH			
a.	* Provide an Initial Government Estimate document.	Appendix P7 - Initial Government Estimate Template	☐ Yes ☐ No
b.	***Provide ***Market Research Results***.	Appendix P6 - Market Research Template	☐ **Yes** ☐ **No**
3. FUNDING DOCUMENTATION			
a.	*Provide *funding document(s)* (e.g., MIPR, PR, etc.): Ensure funding appropriation properly matches the products being procured.	FAR 32.702(a); DFARS 204.7103-1(a)(4) and DoD 7000.14R,Vol 3, Ch 8 Para 080303A	☐ Yes ☐ No

	DOCUMENTATION	REFERENCE	Check if Complete. Answer Yes/No/N/A Where Appropriate
b.	*Provide *Wide Area Workflow* Inspector Code (user must confirm within 5 days of award).		☐ Yes ☐ No
4. REQUIREMENTS			
a.	Ensure you read Appendix 15 Approved Products Lists.	Appendix 15 Approved Products List	☐ Yes ☐ No
b.	*Provide a SOO/TRP.	Appendix P2 - Statement of Objective/Technical Requirements Package, According to ESO-123 section 1.a.2.	☐ Yes ☐ No
c.	Please use the Buying Standards and Specifications to assist in defining minimum performance specifications and standards.	Appendix P3 - Products Buying Standards and Specifications	☐ Yes ☐ No ☐ N/A
d.	Do you require a name brand/specific brand?	FAR 16.505(a) (4) Appendix P13	☐ Yes ☐ No ☐ N/A
e.	Do you have any other *Attachments* that need to be provided (e.g., network topologies, architecture diagrams, etc.)?		☐ Yes ☐ No ☐ N/A
f.	Will you be buying software?	Appendix P5 - Frequently Asked Questions	☐ Yes ☐ No ☐ N/A
g.	*Provide Ozone Depleting Substance Certificate or Letter stating N/A. Provide either the certification that there is no Class 1 ODS or a copy of the GO/SES approval for use of Class 1 ODS.	Appendix P11- Ozone Statement AFFARS 5323.804(b).	☐ Yes ☐ No
h.	*Need Date NOTE: Please see section 5.1 of Appendix P2 - for maximum delivery times	Appendix P2 - Statement of Objective/Technical Requirements package	☐ Yes ☐ No

	DOCUMENTATION	REFERENCE	Check if Complete. Answer Yes/No/N/A Where Appropriate
i.	*Mission Essential Requirements – Are your requirements mission essential? If yes, they must be identified as such.	DODI 3020.37	☐ Yes ☐ No
j.	*Is your solicitation in support of data server farms or data centers? NOTE: If so, then prior approval from the Air Force CIO, and in some cases the DoD CIO, is required. Copies of guidance can be found on NETCENTS-2 website.	AF Guidance Memo to AFI 33-150 from AF CIO dated 18 Aug 2013 AFWay SAN Notice: Law & DoD Policy on Procurement for Data Servers and Centers	☐ Yes ☐ No
5. EVALUATION CRITERIA			
a.	*Final determination will be made by the CO except for applicable Government Purchase Card purchases.	Appendix P8 - Evaluation Criteria FAR PART 16	☐ Yes ☐ No
6. POST AWARD			
a.	*The *Contractor Performance Assessment Reporting System (CPARS)* is required on NETCENTS-2 DOs that exceed $1M. The Requiring Activity must provide a CPARS Focal Point. This is normally the Contracting Officer Representative (COR).	CPARS Focal Point Name: E-mail: Phone:	☐ Yes ☐ No
b.	Customer survey required for orders less than $1M.	Appendix P12 - Customer Survey Template	☐ Yes ☐ No
c.	Public Disclosure of Information. Does your SOO/TRP contain information that, if released, would be harmful to the government?	FOIA Coordinator Name: E-mail: Physical Address: Bldg 884, 501 E. Moore Drive, MAFB-Gunter Annex, AL 36114.	☐ Yes ☐ No ☐ N/A

Statement of Objective (SOO)/Technical Requirements Package (TRP)

Instructions: You must use this format for your NetCentric Products Delivery Orders (DO).

Save a copy of this template and modify it according to your requirements. Each time a SOO/TRP is accomplished, come back to the User's Guide and download the latest SOO/TRP template. The language, standards, and references will be updated over time.

All text that is within brackets [ ] is information that YOU must provide along with some associated information or instructions.

"NOTES" are instructions with additional guidance and are included in the template and highlighted in yellow. You **MUST** delete these notes prior to completing the final SOO/TRP.

All other language may be modified to better explain specific requirements. Only apply modifications, introduce additional information, or include updates in the event that standards or instructions change, or when deemed necessary by your specific program's or organization's policies.

Do not deviate from the format of this template. Doing so could delay the acquisition of your services or support. Using a standard template will help the offeror know where to look for requirements and will decrease the time required to award DOs.

Appendix P4 of the user's guide contains standards and compliance areas to help ensure the equipment you procure meets all network connection criteria.

[REMEMBER to delete all instructional text contained within brackets and note sections herein when completing your SOO/TRP. It is shown here for instructional purposes only and must not remain part of the final document.]

1. SOO/TRP Template for NetCentric Products Purchases

[Provide Requesting Agency name and DO Title]

2. Purpose

[In this short paragraph, briefly define the overall purpose and objective of your requirements]

3. Baseline CLINs for the NetCentric Products Firm Fixed Price (FFP) Contracts

Base Year CLIN structure good for 3 years from award date	Option Year One CLIN #	Option Year Two CLIN #	Option Year Three CLIN #	Description
0100	1100	2100	3100	Networking Equipment
0200	1200	2200	3200	Servers/Storage
0300	1300	2300	3300	Peripherals
0400	1400	2400	3400	Multimedia
0500	1500	2500	3500	Software
0600	1600	2600	3600	Identity Mgt/Biometric Hardware/Software
0700	1700	2700	3700	Data ***Data is not separately priced***
0800	1800	2800	3800	Warranty
0900	1900	2900	3900	Maintenance

NOTE 1: Select the CLIN(s) above that this SOO/TRP is executing against from the overarching NetCentric Products contract. Delete those CLINS not required for this order. If you are not sure which CLIN your hardware falls under, use the Networking Equipment CLIN. This part of the template is just to choose the correct CLINS. You will list your detailed product requirements in section 5.0 of this document.

NOTE 2: NetCentric Products Categories are defined below to help you understand the types of equipment that make up the various CLIN categories. Once you have selected CLINs from above, please delete the definitions below.

- **Network Equipment** can be defined as but not limited to the following: network devices, appliances, switches, hubs, gateways, routers, firewalls, bridges, repeaters, wireless networking devices, microwave radios (data, voice, video), Land Mobile Radios (LMR), satellite communications terminals, adapters, associated cables, interface cards, multiplexers, Voice over IP (VoIP), modems,

cabinets, converters, and test equipment, proxies, network security appliances and Global Positioning System timing systems.

- **Servers/Storage** can be defined as but not limited to the following: low-end servers (tower, rack-mount), medium-end servers (tower, rack-mount, blade), high-end servers (tower, rack-mount, blade), operating systems including, but not limited to, Exchange Server; Microsoft SMS Server; Windows Server; Linux Enterprise; Red Hat Linux Enterprise; Open VMS; UNIX; Netware; Solaris; UnixWare/OpenServer; VMware; Network Attached Storage (NAS), Storage Area Networking (SAN) devices; hard drive/tape drive array, external hard drives, optical drives, CD, DVD, Tape Storage Media; portable storage devices, and various JBODs (Just a Bunch of Disks/Drives) configuration.

- **Peripherals** can be defined as but not limited to the following: various processors with different clock rates, memory modules and upgrades, video cards, network interface cards, interface adapter cards, expansion bay, internal cables, processor/motherboard upgrades, keyboard/mouse, memory cards, power strips, USB hubs, card readers, speakers, external connection cables, expansion chassis, monitors, power adapters, Wi-Fi adapters, faxes, printers, scanners, peripherals (including monitors), Uninterruptible Power Supplies, Power Distribution Units, Surge Suppressors, power strips, USB hubs, computer speakers, touch pads, data terminals, cameras (Web, Network, Wireless), power adapters/cords, antennas, computer switches, Keyboard/Video/Mouse switches, printers, scanners, standard and touch-screen monitors, keyboards/mice, port replicators, computer (display/input) terminals, disc back-up and replication equipment, message archivers, patch panels, warranty variations, and operating systems/licenses when not covered or provided under other existing Government enterprise agreements.

- **Multimedia** can be defined as but not limited to the following: standalone displays (e.g., plasma screens, HDTVs), video devices, DVD/VCR players, Video Teleconferencing equipment, text devices, audio devices, devices that produce still images, animation, video, and interactive media.

- **Software** can be defined as but not limited to the following: is sold independently of hardware, related to NetCentric mission areas such as Network Management, Network Defense, Server Virtualization, Collaboration, Security, Geo-based, E-learning, Database Performance Tuning, Database Warehousing, and Web Development. Other types of software required may include, but not be limited to, storage, database, messaging, backup/recovery, archiving, compliance, provisioning, patch management, asset management, data visualization, business analytics, information assurance and development tools, and Virtualization software management tools.

- **Identity Management/Biometric Hardware and Associated Software** can be defined as but not limited to the following: Electronic Fingerprint Images, Iris Images, Face Recognition, Hand Geometry, Speaker Recognition (telephony based and web based), Multi-modal Biometric Jump Kit, Smart Card Reader (fingerprint), Fingerprint Reader, Palm Vein Authentication, and Public Key Infrastructure (PKI) / Common Access Card (CAC) devices.

4. Technical Requirements

4.1 Standards

NOTE: Review each of the standards below to determine if they apply to your requirement or List of Materials (LOM). If applicable, add the standard or specification to your products table in section 5 under the Specs/Standards column. Also, leave the applicable paragraph(s) below in the SOO.

If procuring a product without a defined configuration, review Appendix P3 for minimum buying standards for the mostly frequently purchased products.

All links/URLs for the following references are included in Appendix P4 if needed.

4.2 Information Assurance (IA) Technical Considerations

The contractor shall ensure that all applicable Commercial-Off-The-Shelf (COTS) IA and IA-enabled products comply with AFI 33-200, Information Assurance. These products must be Committee on National Security Systems Policy 11 (CNSSP-11) compliant, requiring them to be validated by accredited labs under the National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme or National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) Cryptographic Module Validation Program (CMVP). NOTE: Remove if not applicable. The following are some examples of IA and IA enabled devices: data/network encryptors, intrusion detection devices such as Firewalls, Intrusion Detection System, Authentication Servers, Security Gateways, High Assurance IP encryptor and Virtual Private Networks.

4.3 DoD IPV6 Requirement

The contractor shall ensure all applicable products meet the criteria in DoD IPv6 Standard Profiles for IPv6 Capable Products version 5.0 July 2010 (http://jitc.fhu.disa.mil/apl/ipv6/pdf/disr_ipv6_50.pdf). NOTE: Remove if not applicable. Some example IPV6 mandated products from the DoD IPV6 Standards Profile are listed below:

- Host/Workstations - a desktop or other end-user computer or workstations running a general purpose operating system such as UNIX, Linux, Windows, or a proprietary operations system that is capable of supporting multiple applications
- Network Appliance or Simple Server - Simple end nodes such as cameras, sensors, automation controllers, networked phones or adapters such as Circuit-to-Packet (CTP) devices, typically with an embedded operating system and specialized software for limited applications. A Network Appliance is typically managed by an end-user, but may support more than one concurrent user remotely via a Web browser interface. A Simple Server supports a small number of concurrent clients via a web browser interface or other protocol with a client application. Examples of simple servers are stand-alone network print servers, storage servers, Session Initiation Protocol (SIP)11 servers, a “web camera” appliance that serves pictures via an embedded web server, and a network time server appliance that solely functions to serve NTP requests. Advanced Server - End Nodes with one or more server-side applications (for example Dynamic Host Configuration Protocol (DHCPv6), Domain Name Server (DNS), Network Time Protocol (NTP), E-mail, File Transfer Protocol (FTP), Hypertext Transfer Protocol (HTTP), web server, storage server or database) to support clients in the network.

- Intermediate Nodes – Routers, Switches, IA or IA enabled devices
- IPV6 Capable Software - a product that implements functions available via an IPv6 interface to end-users, network nodes or other software, when installed on an appropriate hardware platform.

4.4 Energy Star

The contractor shall ensure all applicable products must be EnergyStar® compliant per DoDI 4170.11, Executive Order 13221, Energy Star and FAR Part 52.223-153. Refer to http://www.energystar.gov/products and the Department of Energy's Federal Energy Management Program (FEMP) at www.femp.energy.gov/technologies/eep_purchasingspecs.html.
NOTE: Remove if not applicable. The following are some example products that are required to be energy star compliant: computers, displays and monitors, enterprise servers, copiers, digital duplicators, fax/printer machines, printers, scanners, televisions, cordless phones, battery chargers, set-top and cable boxes, and audio and video equipment. For further guidance please see the below URL:
http://www1.eere.energy.gov/femp/technologies/eep_purchasingspecs.html

4.5 Encryption Mandates

The contractor shall ensure that all products that will perform any type of data encryption meet FIPS standards for both information assurance and interoperability testing. For more information on FIPS, go to: http://www.itl.nist.gov/fipspubs/by-num.htm.

4.6 BIOS Mandate

The contractor shall ensure that all applicable products shall be BIOS protection compliant with Section 3.1 "Security Guidelines for System BIOS Implementations of SP 800-147," per DoD CIO, in order to prevent the unauthorized modification of BIOS firmware on computer systems. This mandate is only applicable to x86 and x64 desktops and laptops.
NOTE: This only applies to desktops and laptops that are not within the scope of ITCC. There will be future guidance published by the NIST that will cover servers; however there is no BIOS mandate for servers or wireless devices. Remove if not applicable.

4.7 Biometric Mandate

The contractor shall ensure that all applicable biometric products be built to the DoD Electronic Biometric Transmission Specification (EBTS) latest standard (currently version 3.0). For more information please visit the Biometric Identity Management Agency website at: http://www.biometrics.dod.mil/. NOTE: Remove if not applicable. If using biometric data for capturing personal identification such as fingerprints, which will be used for electronic transmission to the FBI or Office of Personnel Management (OPM), these products SHOULD be certified by the FBI Integrated Automated Fingerprint Identification System (IAFIS) program or there is a risk the biometric data will be rejected. An IAFIS certification guarantees compliance with EBTS and FBI standards. Certified products can be viewed at http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/iafis/iafis_cert. More information can be found in Appendix P10 of the user's guide. The following are example products that fall under the Biometric Mandate: fingerprint readers, facial recognition devices, voice recognition, and retina scanners.

4.8 Special Asset Tagging

The contractor shall provide special asset tags IAW MIL STD-130, DODI 8320.04, Item Unique Identification (IUID) Standards for Tangible Personal Property and DFARS

252.211-7703, Item Identification and Valuation. Per AFI 63-101 and AFPAM 63-128, Program Managers are responsible for ensuring items are marked and registered correctly. Requiring a CDRL to identify IUID items and/or embedded items provides a tracking mechanism and promotes early IUID planning by the contractor. The current list of accepted unique item identifier types is maintained at http://www.acq.osd.mil/dpap/pdi/uid/uii_types.html. All DoD recognized unique identification equivalents are listed at http://www.acq.osd.mil/dpap/pdi/uid/iuid_equivalents.html. Please see Appendix P-14 of the user's guide for a listing of products requiring IUID. Special Asset Tagging can be required when:

- All items for which the Government's unit acquisition cost is $5,000 or more;
- Items for which the Government's unit acquisition cost is less than $5,000, when identified by the requiring activity as DoD serially managed, mission essential or controlled inventory;
- When the Government's unit acquisition cost is less than $5,000 and the requiring activity determines that permanent identification is required;
- Regardless of value, (a) any DoD serially managed subassembly, component, or part embedded within an item and, (b) the parent item that contains the embedded subassembly, component or part.

NOTE: Remove if not applicable. If Special Asset Tagging applies then leave the above statement in your SOO. If you require further guidance on Special Asset Tagging please see DoDI 8320.04 at: http://www.dtic.mil/whs/directives/corres/pdf/832004p.pdf.

4.9 Software Tagging

The contractor shall ensure COTS software items support International Standard for Software Tagging and Identification, ISO/IEC 19770-2, Software Tags when designated as mandatory by the standard. NOTE: Check ISO/IEC 19770-2 to see if Software Tagging applies to this acquisition. Some examples of when software tagging is required are to record unique information about an installed software application or to support software inventory and asset management. For more information please go to http://tagvault.org/ - Remove if not applicable.

4.10 Radio Frequency Identification (RFID)

The contractor shall provide RFID tagging IAW DoD Radio Frequency Identification (RFID) Policy, 30 July 2004 or most current version. NOTE: Check RFID Policy, 30 July 2004 at: https://acc.dau.mil/adl/en- S/142796/file/27748/ RFIDPolicy07-30-2004.pdf to see if Special Asset Tagging applies to this acquisition. Some example uses of RFID are when tags are placed into freights containers, ammunition shipments, or attached to unit level IT equipment to facilitate accountability. Remove if not applicable.

4.11 Section 508 of the Rehabilitation Act

The Contractor shall meet the requirements of the U.S. Access Board's regulations at 36 CFR Part 1194, particularly 1194.22, which implements Section 508 of the Rehabilitation Act of 1973, as amended. Section 508 (as amended) of the Rehabilitation Act of 1973 (20 U.S.C. 794d) established comprehensive requirements to ensure: (1) Federal employees

with disabilities are able to use information technology to do their jobs, and (2) members of the public with disabilities who are seeking information from Federal sources will be able to use information technology to access the information on an equal footing with people who do not have disabilities. NOTE: Remove if not applicable.

4.12 DoD Unified Capabilities Requirements (UCR) 2013

The Contractor shall provide UC approved products. The UCR 2013 specifies the functional requirements, performance objectives and technical specifications for DoD networks that support unified capabilities (UC) and is used to support test, certification, acquisition, connection and operation of these devices. The UCR identifies the minimal functional and performance requirements for products to be placed on the UC Approved Products List (UC APL) found here https://aplits.disa.mil/processAPList.do. The UC APL is a consolidated list of products that have completed interoperability and information assurance certification and is managed by Defense Information Systems Agency (DISA). Products are classified into two categories, network infrastructure and voice, video and data services. NOTE: Remove if not applicable. More information can be found in Appendix P15 of the user's guide.

4.13 Cryptographic Module Validation Program

The contractor shall provide Commercial-Off-The-Shelf (COTS) IA and IA-enabled products that are compliant with the Cryptographic Module Validation Program (CMVP). This standard is applicable to ensure security of sensitive information through the use of validated cryptography modules according to FIPS 140-2. Example products include cryptographic software, telecommunication devices, land mobile radios, routers/switches, VPN devices and firewalls. The APL can be viewed at http://csrc.nist.gov/groups/STM/cmvp/validation.html. NOTE: Remove if not applicable. More information can be found in Appendix P15 of the user's guide.

4.14 Common Criteria Evaluation & Validation Scheme

The contractor shall provide Commercial-Off-The-Shelf (COTS) IA and IA-enabled products that are compliant with the Common Criteria Evaluation & Validation Scheme (CCEVS). This standard is applicable to ensure products acquired for use to protect information on National Security Systems are compliant according to Committee on National Security Systems Policy (CNSSP) 11. CCEVS and CMVP certifications cannot substitute each other but products can have both certifications. Example products include VPN gateways, servers, routers/switches, printers/copiers and software. The APL can be viewed at http://www.niap-ccevs.org/CCEVS_Products/pcl.cfm?tech_name=ALL and http://www.commoncriteriaportal.org/products/#BD. The Common Criteria Portal lists globally certified products and can be used as an equivalent. NOTE: Remove if not applicable. More information can be found in Appendix P15 of the user's guide.

4.15 Federal Identity, Credential and Access Management

The contractor shall provide Commercial-Off-The-Shelf (COTS) IA and IA-enabled products that are compliant with the Federal Identity, Credential and Access Management (FICAM) program. This standard is applicable to ensure products that are part of a Personal Identity Verification (PIV) system is FIPS-201 compliant. PIV systems comprise the access card, reader, issuer software and registration database which includes validating the cryptography to FIPS 140-2 standards. Example products include servers, switches/routers, face/palm recognition devices, software, printers/copiers and enterprise security identity and credential management. The list can be viewed at

http://www.idmanagement.gov/approved-products-list-apl. NOTE: Remove if not applicable. More information can be found in Appendix P15 of the user's guide.

4.16 High Assurance Internet Protocol Encryptor

The contractor shall provide Commercial-Off-The-Shelf (COTS) IA and IA-enabled products that are compliant with the High Assurance Internet Protocol Encryptor (HAIPE) program. This standard is applicable to ensure products acquired for use to protect national security information up to Top Secret are compliant with Committee on National Security Systems Policy (CNSSP) 19 and the UCR 2013. Example products include land mobile radios and various network encryption devices. There is no public available APL. NOTE: Remove if not applicable. More information can be found in Appendix P15 of the user's guide.

4.17 TEMPEST Requirements

The contractor shall provide commercially available TEMPEST-compliant communications and information processing devices as applicable.
NOTE: Remove if not applicable. More information can be found in Appendix P15 of the user's guide. TEMPEST is the code name referring to investigations and studies of compromising emissions security. Emissions security are defined as unintentional intelligence-bearing signals which, if intercepted and analyzed, may disclose the information transmitted, received, handled, or otherwise processed by any information processing equipment. The National Security Agency (NSA) is responsible for the test and certification of TEMPEST products such as monitors, workstations, switches, routers, servers, hard drives and printers. The certified TEMPEST list and examples can be found at http://www.nsa.gov/applications/ia/tempest/index.cfm.

5. Products Order Table Information

a. NOTE: As part of the SOO/TRP, fill out the example table below and remove any categories not needed. Add a line for each item required. A list of Product Baseline Standards and Specifications to assist in purchasing IT equipment can be found in Appendix P3 - Products Buying Standards.

b. NOTE: If you are seeking vendor specific hardware, you must file a Fair Opportunity Exception FAR 16.505(a) (4) using a format similar to the J&A information found in 6.302-1(c). See Appendix P13 for a Fair Opportunity Exception (Brand Name Justification Template).

The Contractor shall provide and deliver all products listed and ensure compliance with the associated standards and/or specifications as defined below.

5.0 Products Order Table

Category	List Item Description	Specs/Stand	Special Asset Tagging Required	Quantity
Network Equipment	Example: Wireless Router	Example: Operates on 2.4 – 5 GHz simultaneously, IEEE standard 802.11n	See Section 4.9	4
Servers/Storage	Example: Data Center Class (LAN)	Example: Blade, IPV6 Use at a min 550 Gbps per slot of bandwidth in a 10-slot chassis. Ports can vary based on requirements and can range from 32-10GE or 384 1/10GE ports. POE is required.		5
Peripherals	Example: Printer Plotter	Example: 5 color, 24 inch, minimum resolution 2400x1200, Windows 7 64 bit compatible, roll feed paper, direct PC plug in		1
Multimedia	Example: HD Monitor	Example: Min 27" display, 1920x1080 resolution, maximum response time 5ms (GTG), audio speaker, min 2 each VGA, HDMI and video inputs		9
Software	Example: eLearning Software	Example: Windows 7, content delivery in Flash or HTML, convert MS PowerPoint, custom coding in HTML, JavaScript and XML.		3
Identity Mgt/Biometric Hardware/Software	Example: Fingerprint Scanner/Reader	Example: Performs single or two finger flat roll prints, min 550ppi, FBI IAFIS Certified, FIPS 140-2 Certified, Windows 7 compatible, portable.		6
Warranty	Example: Enhanced Warranty	Example: Provide 24x7 telephone support , 72 hour response for maintenance calls, repair or replace any parts with new or previously used parts, replacement parts are warranted for 2 years of installation even if beyond enhanced warranty period, customer self repair parts will be shipped next business day delivery.		15
Maintenance (rarely used – not for labor hours to do maintenance)	Example: Monthly Maintenance for Dragon Breathalyzer	Example: Perform monthly calibration, software upgrades as needed, restock mouth pieces to minimum 100 on hand and maintain records.		

NOTE: If you cannot determine the category for your IT purchase, please put it under the Networking Equipment then delete this statement, i.e., LMRs.

6. Technical Contractual Requirements

6.1 Hardware and Associated Software and Peripherals

All hardware delivered under this DO shall include associated software, documentation and associated peripherals required for operations (such as controllers, connectors, cables, drivers, adapters, etc.) as provided by the OEM. This is true only if the applicable OEM provides such items with the product itself.

NOTE: Cannot be removed or modified if purchasing hardware.

6.2 Safeguarding Classified Information

The contractor shall transmit and deliver classified material/reports IAW the National Industrial Security Program Operations Manual (NISPOM) and the National Industrial Security Program Operating Manual (DoD 5220.22-M). These requirements shall be accomplished as specified in the Delivery Order. All Classified Contracts must have at a

minimum, the Clause 52.204-2 Security Requirement, incorporated into the contract. NOTE: Remove if not applicable.

6.3 Authorized Resellers

The contractor may be an authorized reseller of new and refurbished/remanufactured equipment for OEMs proposed under this DO. The contractor may also procure directly from the OEM or utilize other legitimate distribution channels to provide the required products. Any contractor's channel relationships with their OEM partners (gold, silver, etc.) will be represented in the best pricing offered. DOs may restrict the use of authorized resellers, specific OEMs, or identify required OEMs. Any product offering that is remanufactured or refurbished shall be clearly identified as such by the contractor. Remanufactured products shall have the OEM or factory certification if available for that product.
NOTE: Cannot be removed or modified if purchasing refurbished or remanufactured items.

6.4 Technical Refresh

In order to ensure new design enhancements and technological updates or advances, the contractor shall offer, under this DO, hardware and software components available to the contractor's commercial customers. Furthermore, the contractor shall make available any commercially available updates to the hardware and software provided under this DO. If such updates are available to other customers without charge, then they shall also be made available to the Government without additional charge. The contractor will ship these updates to existing customers who have acquired the hardware/software being updated under this DO. Vendor commercial product offerings shall include "state of the art" technology, i.e., the most current proven level of development available in each product category. NOTE: Do not remove.

6.5 Trade Agreement Act (TAA)

All proposed products must be compliant with the Trade Agreements Act of 1979 (TAA) and related clauses in Section I of this contract. In accordance with DFARS 252.225-7021, the Trade Agreements Certificate at DFARS 252.225-7020 shall be provided for each end item defined and specified in a solicitation that exceeds the TAA threshold subject to the waivers and exceptions provided in FAR 25.4, and DFARS 225.4 offered in response to any RFQ issued under this contract. Please note that Federal Acquisition Regulation (FAR) paragraph 25.103(e) includes an exemption from the Buy American Act (BAA) for acquisition of information technology that is commercial items. NOTE: Do not remove.

6.6 Items on Backorder

In their response to a Request for Quote (RFQ), the contractor shall provide notification, if applicable, that a particular item is on backorder, the expected lead-time to fulfill the order, etc. It shall be implicit that a response to an RFQ with no items identified on backorder is a declaration that the items are available at the time of quote submission. NOTE: Do not remove.

6.7 Installation

The only time that installation services can be procured is when the services and cost are included in the price of the product as sold commercially. In the rare instances where installation services are required/offered, the contractor shall provide installation support related to the applicable products(s) as defined in the DO. In those instances, the DD Form 254 (DEPARTMENT OF DEFENSE CONTRACT SECURITY CLASSIFICATION

SPECIFICATION) requirements will be addressed in the individual DO and only at the security level necessary. NOTE: Remove if not applicable.

6.8 Warranty

The contractor shall provide any OEM pass through warranty and standard commercial warranties applicable to the products being purchased at no cost. This shall apply to new, refurbished and remanufactured equipment. NOTE: Do not remove. If you need to purchase extended warranties, add the appropriate CLIN to the Product Order Table in section 6.

6.9 Customer Support

The prime contractor shall provide 24x7 live telephone support during the warranty period to assist in isolating, identifying, and repairing software and hardware failures, or to act as liaison with the manufacturer in the event that the customer requires assistance in contacting or dealing with the manufacturer. NOTE: Do not remove.

6.10 Product Maintenance

The contractor shall provide associated maintenance and upgrades to include spares/parts and emergency support worldwide, during the warranty period. NOTE: Do not remove.

7. Delivery Requirements

7.1 Timeframes

NOTE: Choose your delivery requirements based on the table below. The delivery times defined below cannot be modified.

The contractor shall adhere to the following Product Delivery Capability requirements when providing products under this DO. The contractor shall deliver the quantities of NetCentric products to meet ordinary as well as fluctuating (war-time, Terrorist Tempo, Ops Tempo) government requirements in accordance with prescribed delivery schedules stipulated in individual DOs. Delivery of products will be to CONUS, OCONUS, and remote locations as identified below. For AOR's and/or remote sites that do not permit commercial deliveries, the vendor's delivery capabilities must be in accordance with AFI 24-203, Preparation and Movement of Air Force Cargo, 13 April 2007. Additional delivery terms or schedules, such as ship-in-place, expedited shipping or shipping to APO/FPO addresses, shall be negotiated between the Contractor and the Ordering Contracting Officer (OCO).

Definitions: CONUS: The 48 contiguous states, Alaska, Hawaii, and the District of Columbia. OCONUS: Germany, Italy, Japan, Korea, Belgium, Turkey, Puerto Rico, United Kingdom, and the Netherlands. Remote OCONUS: those locations that are not listed under CONUS or Named OCONUS.

The following figure 1 sets forth the maximum performance parameters for deliveries:

Timeframe	CONUS	OCONUS	Remote OCONUS
Routine	NLT 30 calendar days	NLT 45 calendar days	NLT 45 calendar days
Critical	NLT 3 calendar days	NLT 5 calendar days	NLT 10 calendar days
Emergency/War Tempo	Within 24 hours	Within 48 hours	Within 72 hours

Figure 1 - Delivery Performance Parameters

7.2 DO Order Shipping Date

This DO requires a [Insert delivery requirements here. Use either text or a table.
[Example: Routine CONUS order required within 25 days of DO award.]

7.3 Delivery Delays

Contractors are required to meet the timeframes as stated in section 7.1 unless Department of Commerce approval and/or review activities prevent the contractor from meeting these timeframes. In the event that the contractor determines they are unable to achieve the stated timeframes, the contractor shall notify the Contracting Officer within two (2) business days of such determination, or immediately upon such determination if operating under the Emergency/War Tempo timelines. NOTE: Cannot be removed.

7.4 Shipping Information

All products shall be shipped to:
[Insert mailing address]

Inspection/Acceptance: The following Government officials are responsible for receiving the products and performing inspection:
[Primary POC: SSgt John Doe]
[Alternate POC: SrA John Doe]