

Purchase Request Number: CISCOARMY

Justification for Other Than Full and Open Competition (OTFAOC)

Justification for OTFAOC Number: JA12-091

Upon the basis of the following justification, I, as Senior Procurement Executive (SPE) of Defense Information Systems Agency (DISA), hereby approve the use of other than full and open competition of the proposed contractual action pursuant to the authority of 10 U.S.C. §2304 (c)(1). The regulatory authority that applies to the requirement is FAR Part 6.302-1, Only One Responsible Source and No Other Supplies or Services Will Satisfy Agency Requirements.

JUSTIFICATION

1. REQUIRING AGENCY AND CONTRACTING OFFICE:

Requiring Agency:

United States (US) Army Chief Information Office (CIO)/G-6
Pentagon
Washington, DC 20310

Contracting Office:

Defense Information Technology Contracting Organization (DITCO)/PL8321
2300 East Drive, Building 3600
Scott AFB, IL 62225

2. NATURE/DESCRIPTION OF ACTION(S):

a. The purpose of this action is to procure Brand Name Commercial Off-The-Shelf (COTS) Cisco hardware and software maintenance, commonly known as SMARTnet. This acquisition provides for the procurement of new licenses and/or additional licenses, upgrades existing product, and twenty-four (24) hours a day, seven (7) days a week support (24x7). The new contract will perpetuate existing coverage currently provided under multiple contracts with varying periods of performance. The new contract will consolidate maintenance for over 400,000 pieces of Cisco equipment and reduce administration of over 5,000 separate Cisco SMARTnet contracts. Cisco hardware and software encompasses 80% of the Army's network routing and switching capability and has been in place for over ten years. Under this vehicle, SMARTnet services will provide the required maintenance support for all Cisco hardware and software for the US Army. This contract will also procure an Inventory Collection, Reporting and Analysis (ICRA) System in order to manage the inventory of over 400,000 pieces of Cisco equipment. The ICRA will connect directly to the Cisco database to allow for near real-time reporting of Army assets under management. The recommendation is to acquire the SMARTnet maintenance and licensing for the requested products and the ICRA from a Cisco Federal Gold Small Business reseller. This requirement is for a Firm-Fixed Price (FFP) contract utilizing commercial open market procedures.

b. The period of performance (PoP) will consist of a one-year base period and four one-year option periods, for a total contract life cycle of five (5) years. The PoP for the base year will be 29 June 2012 through 28 June 2013 and each option year to follow consecutively through 28 June 2017. Fiscal year 2012 (FY12) Operation and Maintenance Army (OMA) and Procurement funds will be provided using a Military Interdepartmental Purchase Request (MIPR) number. The applicable North American Industry Classification System (NAICS) code is 541519 (size standard 150 employees).

3. DESCRIPTION OF SUPPLIES/SERVICES:

a. The objective of this contracting effort is to provide flexibility and a scope of service sufficient to meet current and future Cisco SMARTnet workloads, security, and modernization requirements, while ensuring the Army receives uninterrupted, continuous access to their applications and data. The Army has made a significant investment in the currently installed Cisco infrastructure to ensure the network's security posture remains accredited. This acquisition will provide brand name maintenance support for the entire Army enterprise, excluding Army Medical Command (MEDCOM), who is supported by Military Health Services (MHS) and US Army Special Operations Command, who is supported by US Special Operations Command (SOCOM).

b. This acquisition will provide brand name SMARTnet Support through a Cisco Gold Certified Partner. Gold Partners are the only ones that meet the Army's requirement of 24x7 as Internetwork Operating System (IOS) updates are only available from a Cisco Federal Gold Partner. Gold Partners have specialization requirements meeting the Army's complexity and ensuring the Army's infrastructure remains operational. They include: Advance Unified Communication, Advanced Routing and Switching, Advanced Security, and Advanced Wireless Local Area Network (LAN). Given the size and complexity of the Army's network, these certifications ensure the resellers have the skills necessary to maintain the Army's infrastructure.

c. Cisco SMARTnet consists of regularly recurring maintenance, updates, revisions, error detection and correction, and rights to new releases and/or versions. All software maintenance consists of patch releases and voice telephone and email access 24x7 via the Technical Assistance Center (TAC). Hardware maintenance consists of:

1. TAC: Provides engineering support which allows Army customers to receive telephonic troubleshooting 24x7 with certified Cisco network experts in voice, video, and data communications networking technology.
2. Cisco.com: Cisco website that provides 24-hour access to the online product and technology information, interactive network management, and troubleshooting tools.
3. IOS: Provides major and minor updates for licensed IOS feature sets. This allows the Army to extend the useful life of its hardware investment by increasing current functionality and ensuring compliance with network security policies and regulations
4. Advanced Hardware Support: Provides 8x5 Next Business Day (NBD) replacement of defective hardware, minimizing potential network down-time.

d. An Inventory Collection, Reporting and Analysis (ICRA) System is being acquired by Army CIO/G-6 in order to manage the inventory of over 400,000 pieces of Cisco equipment. The management of enterprise agreements has been incorporated into Army process and policy for many years. In support of this acquisition, the Army will issue a new moratorium under the Army Federal Acquisition Regulation Supplement on all Cisco SMARTnet procurements. This database and corresponding user interface will be tied to Cisco systems so that as new equipment is acquired, either for life cycle replacement or new capabilities, maintenance for that equipment will be identified for inclusion in the Agreement. The user interface will provide Army users with the ability to review inventory for a subset of the Army's installed base. It will also allow users to make updates to the inventory listing based on equipment moves, adds, transfers, or deletions. This requirement is critical to accomplishing an inventory true-up to verify the Army's current Installed Base value.

e. The scope of the proposed contract addresses the known baseline inventory of Cisco products as identified in the attached Addendum 1 – equipment list. During the Period of Performance (PoP), to include all options, the scope would allow additional quantities for software licenses, hardware, and maintenance support. In addition, the contractor will provide the Army, in this contract, the ability to reduce the maintenance for the expiration of licenses/units, reduction in software product, and/or removal of hardware products from Cisco. The Army may increase and decrease products as the customer requirement dictates, not exceeding the ceiling set forth in this document. An installed base value true-up will allow the Army to fluctuate upward or downward depending upon the Cisco inventory reconciliation/true-up that occurs annually. Purchase of new SMARTnet service may increase the licensing and maintenance cost, whereas end-of-life Cisco equipment may reduce the licensing and maintenance cost.

f. The PoP and estimated value for the lifecycle of this action is as follows:

Base Year	29 June 2012 through 28 June 2013
Option Year 1	29 June 2013 through 28 June 2014
Option Year 2	29 June 2014 through 28 June 2015
Option Year 3	29 June 2015 through 28 June 2016
Option Year 4	29 June 2016 through 28 June 2017
Lifecycle	

4. IDENTIFICATION OF STATUTORY AUTHORITY:

This acquisition is conducted under the statutory authority of 10 U.S.C§2304 (c)(1), and the regulatory authority of FAR 6.302-1/DFAR 206.302-1. Only one responsible source and no other supplies or services will satisfy agency requirements. The items/services are peculiar to one manufacturer's brand name. Only the original equipment manufacturer (OEM)/Cisco or its authorized resellers will satisfy the requirement. No other vendor or distributor can legally obtain access to the software nor can they make duplicate copies, since it is protected by copyright and patent laws.

5. DEMONSTRATION OF CONTRACTOR'S UNIQUE QUALIFICATIONS:

a. Cisco SMARTnet software is fully implemented and integrated into the Army's architecture and has been for more than 10 years. Army's Information Assurance (IA) regulations require each device operating on the Army's network to have the latest software updates to defend against potential security threats, and Functional areas require software and hardware replacement in the event a device fails. The purchase of proprietary software licenses and maintenance, as well as hardware maintenance for the products is required to meet the Army regulation. To duplicate another functional replacement initiative through full and open competition is not in the best interest of the Government at this time in terms of both costs and efficiency. The Army relies almost exclusively on the fully implemented Cisco software and hardware to provide its network routing and switching capability. To procure and rewrite applications to function with replacement products throughout the Army at this time would result in substantial work interruptions creating unnecessary obstacles, restraints, and losses in efficiency. In terms of cost, the Army has invested \$4.2 billion into Cisco hardware and software capabilities. If the Government is required to replace the existing Cisco architecture, the Government would lose its current investment in the existing Cisco products and as a result would have to fund the required installation and deployment of a new system, which would be cost prohibitive. Not only would the money invested be lost, but also time and resources would be strained as outlined below.

b. The proposed acquisition is for continued brand name support in order to maintain uniformity and common troubleshooting and service techniques. Introducing a new manufacturer to service Cisco hardware will not only void the warranties associated with Cisco products currently in place, but it will create an unacceptable security environment for the network by eliminating security updates to essential Cisco network components, placing the reliability of the network at high risk. Due to the criticality of the equipment, as security threats are identified, updates to the IOS must be made. If the network were to fail due to software and hardware failure, day to day work functions, online collaboration, Video Teleconferencing (VTC) capability, and Command and Control of forces in the field would be severely degraded. Only authorized Cisco or authorized resellers can maintain Cisco equipment in order to preserve the warranties and ensure critical security updates are timely provided to the Government.

c. In order to ensure the Army's secured network is not comprised, it is critical for Cisco devices to be kept current with the latest software available, which is only available through the Cisco SMARTnet maintenance support. Nearly all Cisco hardware is operated by an IOS, which allows the user to configure the equipment and to control flow of information and establish security protocols. The IOS updates are mandatory for ensuring Army's security posture. As with most IT equipment, the Cisco equipment currently installed requires frequent updates to patch security vulnerabilities. The devices cannot be legally patched without SMARTnet or the purchase of individual updates from Cisco or its resellers, which would be much more expensive and cost prohibitive given the size of the Army's network. All Critical Information Assurance Vulnerability Assessments (IAVA) require immediate remediation; and lack of SMARTnet would prevent the Army from applying the necessary patches, creating significant security implications in a timely manner. Access to additional resources for problem troubleshooting will minimize network outages and ensure security of the data being transmitted. The cost to remediate a single network compromise on an individual basis would not provide timely incident resolutions and would cost more than \$150B. While federal security breaches are classified, there are many public examples including the recent attacks on Sony and Citibank. Successful

attacks on un-patched software have caused billions of dollars in damage, in both private and public sectors. The IAVA policy requires Department of Defense (DoD) Components to register with the IAVA database and report compliance to IAVA notifications. The compliance information must be reported by stating the number of assets affected, in compliance, and with waivers. Failure to properly patch affected systems will violate Army policy in accordance with Army Regulation 25-2 as well as other related policies and could result in service disruption and/or breaches in network security. Purchase of Cisco SMARTnet support and the ICRA is the only option for meeting these requirements.

d. SMARTnet support is also critical to maintaining the Army Global Network Enterprise (GNE). The GNE integrates several ongoing network enterprise programs and new initiatives into a single strategy to ensure global connectivity under one network manager. Using GNE to organize the Army's information will make it globally accessible and useful to soldiers worldwide. The GNE is an Army-wide strategy to operationalize LandWarNet as an Army enterprise activity. The GNE is an integrating construct to bring LandWarNet and battle command programs and initiatives into theater-based alignment with this enterprise objective. The GNE similarly relies upon existing Cisco architecture. As a result, the same costs and security risks discussed above apply to the GNE if other than Cisco SMARTnet support is provided.