JUSTIFICATION REVIEW DOCUMENT

CONTROL NUMBER: HQC007-12-02
PURCHASE REQUEST: HQCAAA-1312-2100

Description of Acquisition: This requirement is to purchase Intrusion Prevention Sourcefire hardware, software and maintenance.

Statutory Authority: 10 U.S.C. 2304(c)(1) as implemented by FAR 6.302-1(c). Application of brand name descriptions

Estimated Contract Amount:

Prepared by:	Jason Nuckols Phone: (804) 734-8000 Ext: 86184	Contract Specialist Date: 11/30/2011
Technical:	Mike Boring MB Phone:	Program Manager Date: 11-30-2011
BEIMG Rep:	Anthony Mertens Phone:	IT Specialist Date: 11-30-2011
PCO:	Rita W. Jackson RWJ Phone: (804) 734-8000 Ext: 48199	Contracting Officer Date: 11/30/2011

REVIEWS: We have reviewed this J&A and find the justification adequate to support other than full and open competition.

Program Manager: Mike Boring

Signature: Mike Boring Date: 11-30-2011

Legal Counsel: Elliot J Clark, Jr.
(Printed Name)

Signature: Elliot J Clark Jr Date: 1 Dec 2011

Competition Advocate: Melissa Rios

Signature: Date: 12/1/11

JUSTIFICATION FOR OTHER THAN FULL AND OPEN COMPETITION APPLICATION OF BRAND NAME DESCRIPTIONS

DECA CONTROL NUMBER: HQC007-12-02

1. REQUIRING AGENCY AND CONTRACTING OFFICE:
Defense Commissary Agency (DeCA)
1300 E Avenue
Fort Lee, VA 23801-1800

Requiring Activity: Information Technology Directorate, Technology Enhancement Branch (BEIT)
Contracting Activity: Store Services Support Division, Information Technology Branch

2. NATURE/DESCRIPTION OF ACTION(S). This justification for other than full and open competition will result in award of a firm fixed price contract for brand name hardware, software and maintenance support for the agency's Intrusion Prevention System (IPS).

3. DESCRIPTION OF SUPPLIES/SERVICES. This requirement is to purchase brand name Sourcefire hardware, software, and maintenance support.

Item #	BASE YEAR DESCRIPTION	P/N	Qty
1	Sourcefire 3D2000 w/IPS 4 Port Copper with Fail Open	3D2000-IPS-C04-000	8
2	Sourcefire Support-SF 3D2000 IPS FO QPC-Gold	S-3D2000-IPS-C04-000-G	8
3	Sourcefire 3D1000 with IPS FO, QPC, 45 Mbps	3D1000-IPS-C04-000	4
4	Sourcefire Support-SF 3D1000 IPS FO QPC-Gold	S-3D1000-IPS-C04-000-G	4
5	Sourcefire 3D500 w/IPS 4 Port Copper with Fail Open	3D500-IPS-C04-000	1
6	Maintenance 3D500 IPS FO QPC Gold	S-3D500-IPS-C04-000-G	1
7	Sourcefire DC1000 Bundled with 500 RNA & 2500 RUA Licenses	DC1000-000-000-C-0-W-RNARUA	1
8	Sourcefire Gold Support for S-DC1000-000-000-C-0-W-RNARUA - 1 YR	S-DC1000-000-000-C-0-W-RNARUABU	1
9	Rackmount Shelf for 3D500, 3D1000, & 3D2000	3D-PB-Rack-Kit	13
10	Deployment Support for 3 Days	PS-PRD-DEP-3 (Not Separately Priced)	1
11	Travel and Expenses	TRN-Travel-Expenses (Not Separately Priced)	1

Item #	OPTION YEAR 1 DESCRIPTIONS	P/N	QYT
2	Sourcefire Support-SF 3D2000 IPS FO QPC-Gold	S-3D2000-IPS-C04-000-G	8
4	Sourcefire Support-SF 3D1000 IPS FO QPC-Gold	S-3D1000-IPS-C04-000-G	4
6	Maintenance 3D500 IPS FO QPC Gold	S-3D500-IPS-C04-000-G	1
8	Sourcefire Gold Support for S-DC1000-000-000-C-0-W-RNARUA - 1 YR	S-DC1000-000-000-C-0-W-RNARUABU	1

Item #	OPTION YEAR 2 DESCRIPTIONS	P/N	QYT
2	Sourcefire Support-SF 3D2000 IPS FO QPC-Gold	S-3D2000-IPS-C04-000-G	8
4	Sourcefire Support-SF 3D1000 IPS FO QPC-Gold	S-3D1000-IPS-C04-000-G	4
6	Maintenance 3D500 IPS FO QPC Gold	S-3D500-IPS-C04-000-G	1
8	Sourcefire Gold Support for S-DC1000-000-000-C-0-W-RNARUA - 1 YR	S-DC1000-000-000-C-0-W-RNARUABU	1

The period of performance includes a 12.5-month base period and two 12-month option periods, if exercised, for a total of three years as follows:

Base Year: December 12, 2011 – December 31, 2012
Option Year One: January 01, 2013 – December 31, 2013
Option Year Two: January 01, 2014 – December 31, 2014

4. IDENTIFICATION OF STATUTORY AUTHORITY.

10 U.S.C. 2304(c)(1) as implemented by FAR 6.302-1(c). Application of brand name descriptions the Brand Name hardware, software and maintenance support

5. IDENTIFICATION OF JUSTIFICATION RATIONALE.

The Department of Defense Directive (DoDD) O-8530.1 requires that all Department of Defense (DoD) Components establish or subscribe to Computer Network Defense Service Provider (CNDSP). DeCA established a Computer Network Defense (CND) Program and was certified as a Tier 2 General Service (GENSER) Provider by United States Strategic Command (USSTRATCOM) in May 2009. One of the many requirements of DoDD O-8530.1 is that all DoD systems and networks be monitored by Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) at every ingress and egress point. Situational awareness of the activity on the Global Information Grid is essential to the security of the Nation. To fulfill this mission, the Defense Information Systems Agency (DISA) uses Sourcefire Computer network software to provide visibility of the activity on the Global Information Grid as a Tier 1 provider. DeCA has the same requirement and to facilitate integration and coordination with DISA, has identified Sourcefire as the IDS to fulfill this requirement. This brand of software is requested to maintain uniformity and minimize potential downtime. This will ensure consistency in the architecture design, maintain continuity, ease of use, and ensure interoperability in accordance with DoDDs.

DeCA is currently using an IDS that has reached the end of its life cycle and is one that utilizes proprietary signatures that are not directly compatible with IDS signatures routinely provided by DISA and US Cyber Command Tier 1 CND Providers. Sourcefire is a commercial product based upon Snort, an open source intrusion detection system that has been an industry leader since 1998. Snort signatures are the standard format for US Cyber Command alerts that DeCA must add to the IDS/IPS filters, Snort signatures are created, vetted and supported by a community of over 100K members, Snort signatures are a de facto standard, Snort signatures are intuitive and easy to develop for local applications. Sourcefire can also function as a network sniffer and packet logger. It can generate real-time alerts and is capable of providing analysis and limited interpretation of events. One of its most powerful applications is the ability to implement rules. The rule structure is simple, powerful and flexible, allowing easy customization for local requirements. There are thousands of publicly available rules which can be tailored for use by in-house personnel, thus minimizing the cost of implementation. Sourcefire allows for the detection of vulnerabilities, exploits, or other conditions using a number of different methods. Sourcefire also supports Internet Protocol version 6 and standardized logging, and has an excellent set of instructional, training, and reference material available.

Sourcefire is National Information Assurance Program (NIAP) Evaluation Assurance Level (EAL)-2 certified and was competitively acquired by the Defense Information Technology Contracting Organization (DITCO) Scott Air Force Base as the standard IDS used by all DISA components. A copy of DISA's Authorization to Operate for the Sourcefire Intrusion Detection System is provided as additional information. Sourcefire could potentially allow DeCA to eliminate two platforms with a single replacement, since it cover the perimeter resources, the developing virtual server base, and also serve as an anomaly-detection platform. Sourcefire has also been identified by Gartner as a leader in the IDS/IPS marketplace, by SC Magazine (February 15, 2011) as the best IDS/IPS in a 5-way competition between competing IDS/IPS vendors, and by NSS Labs as having the "highest accuracy and throughput tested to date" (April 2011).

Sourcefire is the Original Equipment Manufacturer (OEM) and has proprietary rights to the software code for the products associated with the requirement, as such is the only known vendor, along with its authorized resellers, that can provide the spectrum of required products and support.

6. DETERMINATION OF FAIR AND REASONABLE COST. In accordance with FAR 8.404, 12.209, 13.106-1 (2), and 14.408-2, I hereby determine that the anticipated cost or price to the Government for this contract action will be fair and reasonable. The Price Reasonableness Memorandum detailing the Fair and Reasonable Price Determination will be included in the contract file documentation.

7. MARKET RESEARCH.

Market research consisting of internet searches, trade magazines and information technology articles indicates that there are numerous sources available to offer pricing as both resellers and support providers for the Sourcefire product. GSA and other DoD agency contract vehicles were researched; the particular products/versions are available under existing Government Wide Acquisition Contracts (GWAC).

8. ANY OTHER SUPPORTING FACTS:

While the agency seeks to procure this requirement under FAR Part 6.302-1(c), application of brand name descriptions, a number of resellers and support providers have been identified that are able to fulfill this requirement; therefore, adequate price competition is expected.

9. ACTIONS TAKEN TO REMOVE BARRIERS TO COMPEITION:

DeCA continues to perform market research for products that are available and designed to run on open platforms and through virtualization in lieu of the old legacy closed platforms. DeCA continually communicates and works with other DoD agencies, its business partners, and attends trade and industry shows, in an effort to stay abreast of this evolving technology. As legislation and regulatory changes mandated by DoD change and influence the DoD department's information technology requirements, the commercial market place's ability to stay abreast of those changes and provide viable solutions will also change.

10. TECHNICAL CERTIFICATION: "I certify that the supporting data under my cognizance which are included in the J&A are accurate and complete to the best of my knowledge and belief."

NAME: Mike Boring SIGNATURE: Mike B

TITLE: Program Manager DATE: 11-30-2011

CONTRACTING OFFICER CERTIFICATION: "I have reviewed this justification and find it to be accurate and complete to the best of my knowledge and belief. Since this justification does not exceed $550,000 and pursuant to the authority of 10 U.S.C. 2304(c)(1) provided that funds are available or will be made available and provided that the services and/or supplies herein described have otherwise been authorized for acquisition, this review serves as approval."

NAME: Rita W. Jackson SIGNATURE: *Rita W. Jackson*

TITLE: Contracting Officer DATE: 11/30/2011

DEFENSE INFORMATION SYSTEMS AGENCY
P.O. Box 4502
ARLINGTON, VIRGINIA 22204-4502

IN REPLY REFER TO: Chief Information Officer (CIO) JUN 16 2009

MEMORANDUM FOR DIRECTOR FOR INFORMATION ASSURANCE AND NETWORK OPERATIONS (PEO-IAN)

SUBJECT: Authorization to Operate for the Sourcefire Intrusion Detection System, Tracking Number 14650405, DITPR ID 11028

References: (a) DISA Memo, SPI, Appointment of Designated Approving Authority for DISA Information Technology, 8 February 2006
(b) DISA Instruction 630-230-19, Information Assurance, 2 March 2007
(c) DoD Instruction 8510.01 DoD Information Assurance Certification and Accreditation Process (DIACAP), 28 November 2007
(d) DISA Memo, CIO, Second Extension to the Interim Authorization to Operate for the Sourcefire Intrusion Detection System, Tracking Number 14650405, 18 December 2008
(e) DISA IM, FS, Certification and NetOps Readiness Recommendation for Sourcefire (CA: 09D-A-05-163-U/C / TN: 14650405), 28 May 2009

1. In accordance with provisions set forth in references (a) through (c), and based on review of references (d) and (e), an Authorization to Operate (ATO) is issued to the Sourcefire Intrusion Detection System (IDS). This system is authorized to process information up to and including Controlled Unclassified Information (CUI) in a System High mode of operation when connected to the Unclassified but Sensitive Internet Protocol Router Network (NIPRNet) and up to and including SECRET in a System High mode of operation when connected to the Secret Internet Protocol Router Network (SIPRNet). Although component-level Cat I findings exist, these weaknesses are offset and/or mitigated by other protections within the hosting enclave so that the overall risk to the system is reduced to a Cat II. This ATO expires three years from the date of this memorandum.

2. The scope of this ATO includes the Sourcefire Management Consoles for central management, located at Defense Enterprise Computing Center (DECC) Processing Element (PE) Warner-Robins AFB as well as the Sourcefire IDS sensors.

3. This Type approved configuration means Sourcefire IDS sensors can be implemented at other sites with minimal time, effort, and resources, providing the implementation is in compliance with the approved type baseline.

4. New sites must submit a statement of compliance with the Sourcefire IDS baseline accreditation to the Program Manager (PM) and the Designated Accrediting Authority (DAA) Representative (CI32) once installation is complete. New sites must also update their site DoD Information Assurance Certification and Accreditation Process (DIACAP) artifacts to include Sourcefire IDS within the site. The PM must ensure separate Certification and Accreditation efforts are conducted for those systems found not compliant with the baseline configuration.

5. Sites external to DISA must coordinate installation and operational approval with the appropriate DAA.

6. During the period of this ATO, the Sourcefire PM must ensure the security posture of the system is not degraded in any way. Required actions for the PM during the period of this ATO include:

a. Continue to coordinate with Field Security Operations (FSO) to close open findings and ensure identified findings are properly annotated in the Vulnerability Management System (VMS) and remediation efforts are underway. Coordinate validation of closures with FSO.

b. Continue to update your Plan of Action and Milestones (POA&M) within VMS for all open CAT I and CAT II findings to include estimated completion dates, current mitigating measures, and planned actions to close findings. This is an Office of the Secretary of Defense requirement under the Federal Information Security Management Act of 2002. Updates to the POA&M are due quarterly with your first update due within 90 days of the original POA&M submission. Updates to the POA&M are due quarterly.

c. Continue to update your DoD Information Assurance Certification and Accreditation Process (DIACAP) Comprehensive Package artifact documents. Please direct any questions you might have concerning DIACAP and the Comprehensive Package to CI32.

d. Continue to coordinate with the GIG Global Infrastructure Service Management Center and the JTF-GNO NetOps to schedule your NetOps Readiness review. The NetOps review must be completed no later than 31 March 2010.

e. Sourcefire is a Mission Assurance Category (MAC) III system and as such must comply with MAC III level Information Assurance controls prescribed in Department of Defense Instruction 8500.2, "Information Assurance Implementation." Ensure Sourcefire is compliant with these requirements, as compliance will be validated during annual Security Readiness Reviews.

f. Sourcefire processes information up to and including CUI information when connected to the NIPRNet and information up to and including SECRET when connected to the SIPRNet and as such must comply with Sensitive and Classified Confidentiality level Information Assurance controls prescribed in Department of Defense Instruction 8500.2, "Information Assurance Implementation." Ensure Sourcefire is compliant with these requirements, as compliance will be validated during annual Security Readiness Reviews.

g. Ensure compliance with all operational and security guidance published by the JTF-GNO to include applicable Communications Tasking Orders (CTOs) and Information Assurance Vulnerability Management (IAVM) requirements. This particularly includes monthly scanning and remediation, as detailed in CTO 08-005. Results of these scans must be uploaded into the VMS and will be used to validate Sourcefire compliance with Security Technical Implementation Guide and IAVM requirements. The PM must consider scan results when updating the POA&M.

h. Ensure compliance with DoD Information Technology Portfolio Repository (DITPR) requirements to include maintenance of the system record within the DITPR database.

h. Ensure Contingency and Continuity of Operations Plans are developed and tested annually. Proof of testing must be provided to this office, CI32, annotated in system accreditation documentation, and documented in the DITPR database.

7. This ATO is contingent upon maintaining an acceptable security risk posture. During the period of this ATO, the Sourcefire IDS PM must immediately contact and coordinate with CI32 on any of the following:

a. Mission requirements to process information higher than SECRET when connected to the SIPRNet and CUI when connected to the NIPRNet are identified.

b. A requirement to modify, add or remove, as appropriate, any NIPRNet or SIPRNet Command Communications Service Designators (CCSD) is identified. In addition to coordination with this office, any action involving CCSD must be compliant with applicable Connection Approval Processes.

c. Changes must be made to the system architecture or configuration not covered in the DIACAP comprehensive package or similar artifacts.

d. The system, or portion thereof, must be relocated to a different environment.

e. Any Category I findings not previously identified in the VMS are identified.

8. Retain this memorandum on file, as it serves as an accreditation decision. Continued accreditation is contingent upon your conducting an annual accreditation baseline review. Submit a copy of the baseline review, to include any changes to the DIACAP artifacts, to this office each year on the anniversary of this memorandum until the system undergoes re-accreditation.

9. Questions may be directed to Ms. Alma Miller, Chief, DISA Information Assurance Division, at (703) 681-4313, DSN 761, cioiase@disa.mil.

Roberta G Stempfley

ROBERTA G. STEMPFLEY
Chief Information Officer

Copy to:
FS1(J. Snouffer, L.Boyer, P. Fedorczyk, D. Glover, L. Gardner)
GO431 (M. Nassif)
IA22 (S. Mapes, R. Henderson)
IA1 (K. Nguyen, R. Robinson)