ORDER FOR SUPPLIES OR SERVICES

1. CONTRACT/PURCH. ORDER/ AGREEMENT NO.	2. DELIVERY ORDER/ CALL NO.	3. DATE OF ORDER/CALL	4. REQ./ PURCH. REQUEST NO.	5. PRIORITY
DCA200-00-D-5021	0025	2004 Sep 24	DGEMZ49877	

6. ISSUED BY CODE HC1013
DISA/DITCO-SCOTT
2300 EAST DRIVE
SCOTT AFB IL 62225-5406

7. ADMINISTERED BY CODE
SEE ITEM 6

8. DELIVERY FOB
[X] DEST
[ ] OTHER
(See Schedule if other)

9. CONTRACTOR CODE 0GS16 FACILITY
DIGITALNET GOVERNMENT SOLUTIONS LLC
TYLER BROOKS-CRAFT
2525 NETWORK PLACE
HERNDON VA 20171-3514

10. DELIVER TO FOB POINT BY (Date)
SEE SCHEDULE

11. MARK IF BUSINESS IS
[ ] SMALL
[ ] SMALL DISADVANTAGED
[ ] WOMEN-OWNED

12. DISCOUNT TERMS

13. MAIL INVOICES TO THE ADDRESS IN BLOCK
See Item 15

14. SHIP TO CODE
SEE SCHEDULE

15. PAYMENT WILL BE MADE BY CODE N68566
DFAS PENSACOLA
MAIL TO: DITCO/AQSC4-FMO
SCOTT AFB IL 62225-5406

MARK ALL PACKAGES AND PAPERS WITH IDENTIFICATION NUMBERS IN BLOCKS 1 AND 2.

16. TYPE OF ORDER

DELIVERY/ CALL	X	This delivery order/call is issued on another Govt. agency or in accordance with and subject to terms and conditions of above numbered contract.
PURCHASE		Reference your quote dated Furnish the following on terms specified herein:

ACCEPTANCE. THE CONTRACTOR HEREBY ACCEPTS THE OFFER REPRESENTED BY THE NUMBERED PURCHASE ORDER AS IT MAY PREVIOUSLY HAVE BEEN OR IS NOW MODIFIED, SUBJECT TO ALL OF THE TERMS AND CONDITIONS SET FORTH, AND AGREES TO PERFORM THE SAME.

NAME OF CONTRACTOR | SIGNATURE | TYPED NAME AND TITLE | DATE SIGNED (YYYYMMMDD)

[ ] If this box is marked, supplier must sign Acceptance and return the following number of copies:

17. ACCOUNTING AND APPROPRIATION DATA/ LOCAL USE
See Schedule

18. ITEM NO.	19. SCHEDULE OF SUPPLIES/ SERVICES	20. QUANTITY ORDERED/ ACCEPTED*	21. UNIT	22. UNIT PRICE	23. AMOUNT
	SEE SCHEDULE				

* If quantity accepted by the Government is same as quantity ordered, indicate by X. If different, enter actual quantity accepted below quantity ordered and encircle.

24. UNITED STATES OF AMERICA
TEL:
EMAIL: iascottafb@scott.disa.mil
BY: ANNE (KAREN) KELLER
Anne K. Keller
CONTRACTING / ORDERING OFFICER

25. TOTAL $10,290,692.02
29. DIFFERENCES

26. QUANTITY IN COLUMN 20 HAS BEEN
[ ] INSPECTED [ ] RECEIVED [ ] ACCEPTED, AND CONFORMS TO THE CONTRACT EXCEPT AS NOTED

DATE | SIGNATURE OF AUTHORIZED GOVT. REP.

27. SHIP NO.
[ ] PARTIAL
[ ] FINAL

28. DO VOUCHER NO.

30. INITIALS

32. PAID BY

33. AMOUNT VERIFIED CORRECT FOR

31. PAYMENT
[ ] COMPLETE
[ ] PARTIAL
[ ] FINAL

34. CHECK NUMBER

35. BILL OF LADING NO.

36. I certify this account is correct and proper for payment.

DATE | SIGNATURE AND TITLE OF CERTIFYING OFFICER

37. RECEIVED AT	38. RECEIVED BY	39. DATE RECEIVED (YYYYMMMDD)	40. TOTAL CONTAINERS	41. S/R ACCOUNT NO.	42. S/R VOUCHER NO.

Section B - Supplies or Services and Prices

ITEM NO	SUPPLIES/SERVICES	MAX QUANTITY	UNIT	UNIT PRICE	MAX AMOUNT
0001		1	Each	$1,233,015.30	$1,233,015.30

Information Assurance Support Services

T&M

Department of Defense (DoD) Wide Enterprise License for an Automated Secure Configuration Remediation Initiative (SCRI) tool support as in accordance wtih SOW dated 20 July 04 which is an attachment to this order. Period of performance of this requirement is from 24 Sep 04 thru 23 Sep 05 as in accordance with DigitalNet proposal dated 20 Aug 04 which is incorporated by reference into this order.

PURCHASE REQUEST NUMBERS: DGEMZ49877 and DGEMZ49895

TOT MAX PRICE	$1,233,015.30
CEILING PRICE	
ACRN AA Funded Amount	$1,233,015.30

FOB: Destination

ITEM NO	SUPPLIES/SERVICES	MAX QUANTITY	UNIT	UNIT PRICE	MAX AMOUNT
0002		1	Each	$8,943,757.18	$8,943,757.18

SERVICES NON PERSONAL

FFP line items for license, training and support:

1) Enterprise License - $7,762,493.58

2) Virtual On-Demand training courseware including 200 seats running on NACON system - $351,244.05

3) Training hardware, software and courser material - $204,892.36

4) Technical Support - $244,361.25

5) 21 Tool Suites for 120 day rapid deployment - $112,543.20

6) Option 1: Classroom training CONUS per seat (50 seats) - $47,896.92

7) Option 2: Classroom training OCONUS per seat (75 seats) - $87,811.01

8) Option 3: Classroom training CONUS per seat (65 seats) - $62,265.99

9) Option 4: Classroom training OCONUS per seat (60 seats) - $70,248.82

TOTAL	$8,943,757.18

FOB: Destination

ITEM NO	SUPPLIES/SERVICES	MAX QUANTITY	UNIT	UNIT PRICE	MAX AMOUNT
0003		1	Each	$113,919.54	$113,919.54
	T&M				
	ODCS - TRAVEL AND LIVING COSTS.				
				TOT MAX PRICE	$113,919.54
				CEILING PRICE	

FOB: Destination

ITEM NO	SUPPLIES/SERVICES	MAX QUANTITY	UNIT	UNIT PRICE	MAX AMOUNT
1001		1	Each	$231,789.00	$231,789.00
	SERVICES NON PERSONAL				
	T&M				
	Option Year 1 - Department of Defense (DoD) Wide Enterprise License for an Automated Secure Configuration Remediation Initiative (SCRI) tool support as in accordance with SOW dated 30 July 04 which is an attachment to this order. Period of performance of Option Year 1 is from 24 Sep 05 thru 23 Sep 06 as in accordance with DigitalNet proposal dated 20 Aug 04 which is incorporated by reference into this order.				
				TOT MAX PRICE	$231,789.00
				CEILING PRICE	
	Funded Amount				$0.00

FOB: Destination

ITEM NO	SUPPLIES/SERVICES	MAX QUANTITY	UNIT	UNIT PRICE	MAX AMOUNT
2001		1	Each	$238,292.00	$238,292.00

SERVICES NON PERSONAL

T&M

Option Year 2 - Department of Defense (DoD) Wide Enterprise License for an Automated Seure Configuration Remediation Initiative (SCRI) Tool support as in accordance with SOW dated 30 July 2004. Period of performance of Option Year 2 is from 24 Sep 06 thru 23 Sep 07 as in accordance with DigitalNet proposal dated 20 Aug 04 which is incorporated by reference into this order.

TOT MAX PRICE	$238,292.00
CEILING PRICE	
Funded Amount	$0.00

FOB: Destination

ITEM NO	SUPPLIES/SERVICES	MAX QUANTITY	UNIT	UNIT PRICE	MAX AMOUNT
3001		1	Each	$244,991.00	$244,991.00

SERVICES NON-PERSONAL

T&M

Option Year 3 - Department of Defense (DoD) Wide Enterprise License for an Automated Secure Configuration Remediation Initiative (SCRI) Tool support as in accordance with SOW dated 30 July 04 which is an attachment to this order. Period of performance of Option Year 3 is from 24 Sep 07 thru 23 Sep 08 as in accordance with DigitalNet proposal dated 20 Aug 04 which is incorporated by reference into this order.

TOT MAX PRICE	$244,991.00
CEILING PRICE	
Funded Amount	$0.00

FOB: Destination

ITEM NO	SUPPLIES/SERVICES	MAX QUANTITY	UNIT	UNIT PRICE	MAX AMOUNT
4001		1	Each	$251,891.00	$251,891.00

SERVICES NON PERSONAL

T&M

Option Year 4 - Department of Defense (DoD) Wide Enterprise License for an Automated Secure Configuration Remediation Initiative (SCRI) tool support as in accordance with SOW dated 30 July 04 which is an attachment to this order. Option Year 4 period of performance of this requirement is from 24 Sep 08 thru 23 Sep 09 as in accordance with DigitalNet proposal dated 20 Aug 04 which is incorporated by reference into this order.

TOT MAX PRICE	$251,891.00
CEILING PRICE	
Funded Amount	$0.00

FOB: Destination

Section G - Contract Administration Data

ACCOUNTING AND APPROPRIATION DATA

AA: 97X4930.5F20 000 C1013 0 068142 2F 255011
AMOUNT: $10,290,692.02 BREAKOUT IS AS FOLLOWS: MIPR DGEMZ49877 - $ 9,803,570.59
MIPR DGEMZ49895 - $ 487,121.43

CLAUSES INCORPORATED BY FULL TEXT

DITCO Points of Contact

Contracting Officer

Contract Specialist

CONTRACTOR Point of Contact

Contractor Name: DigitalNet
DUNS: 175301720
CAGE CODE: OGS16
Contractor POC:
Email Address:
Phone Number:
Fax Number:

Electronic invoices may be sent to:

invoicereceipt@scott.disa.mil

Questions regarding invoices may be directed to (618) 229-9228. Vendors may check the status of invoices at the following web site:

http://www.dfas.mil/money/vendor

CREDIT CARD METHOD OF PAYMENT

If payment is to be made via credit card, contact the Contracting Officer listed above.

Section J - List of Documents, Exhibits and Other Attachments

SOW DATED 30 JULY 2004

‘I ASSURE’ TASK ORDER (TO) STATEMENT OF WORK (SOW) as of 30 /JULY/2004

Contract Number:	*DCA20000D5021*
Task Order Number:	*0025*
I Assure Tracking Number:	*IA00254.00*
Follow-on to I Assure Contract and Task Order Number:	

1. Task Monitors (TMs)

a. Primary TM

Name:	
Organization:	DISA/GE62
Address:	**5275 Leesburg Pike, Falls Church, VA 22041**
Phone Number:	
Fax Number:	
E-Mail Address:	
DODAAC:	

b. Alternate TM

Name:	
Organization:	DISA/GE62
Address:	*5275 Leesburg Pike, Falls Church, VA 22041*
Phone Number:	
Fax Number:	
E-Mail Address:	
DODAAC:	

2. Task Order Title

Department of Defense (DoD)-wide Enterprise License for an automated Secure Configuration Remediation Initiative (SCRI) tool.

3. Background

3.1. Vulnerability Management

Vulnerabilities exist when there is a flaw or weakness in hardware or software that can be exploited resulting in a violation of security policy. Vulnerabilities can be the result of a flaw in the coding of software, configuration, and a great number of other factors. As systems and applications become more complex, the number of lines of code multiplies exponentially. Consequently, the potential for flaws also multiplies. By exploiting vulnerabilities malicious code can cause significant and pervasive damage. Contractors, users, researches, and hackers often discover vulnerabilities in existing systems or applications. To rectify the problem, contractors often issue a short-term fix in the form of a patch or recommended change to protocol or configuration.

While the threat to Department of Defense (DoD) systems cannot be eliminated, the following processes effectively manage the risk associated with vulnerabilities:

- Automated Vulnerability Identification and Reporting
- Automated Vulnerability Remediation
- Field Proven Tools
- Minimally disruptive to Normal Operations
- Accountability and Enforcement
- Training Support for SCRI tool

A critical aspect of effective Computer Network Defense (CND) is ensuring software operating systems and applications are kept up-to-date with the latest vulnerability patch.

3.2. Authority

The Defense Information Systems Agency (DISA), at the request of the United States Strategic Command (USSTRATCOM) and in support of National Security goals established by the President, intends to purchase from industry, a capability that will assist in the development and deployment of an automated SCRI tool that will provide network administrators and security personnel a mechanism for the remediation of vulnerabilities based on DoD instructions. This tool will be the Enterprise-wide solution across the “Department of Defense (DoD) (Combatant Commands, Intelligence Community (non-Title 50 elements), Services, and DoD Agencies), Coast Guard, National Guard, and the Reserves” here after referred to as the “ENTERPRISE”. All “ENTERPRISE” owned and leased computers and networks are covered under this agreement, regardless of the persons operating the computer systems. This capability should fully integrate IA vulnerability remediation while providing a cost effective training method to employ the technology. Emphasis should include the capability to employ these tools in all operating environments, such as specified in the Common Operating Environment (COE).

4.0 TECHNICAL REQUIREMENTS

4.1 OBJECTIVE

This SCRI effort is to provide an ENTERPRISE-wide automated standardized tool to remediate emerging and known IA vulnerabilities at the asset level.

4.1.1 INTEROPERABILITY REQUIREMENTS

4.1.1.1 The system shall accept the input from the Secure Configuration Compliance Validation Initiative (SCCVI) tool. This tool is the eEye Digital Security Retina suite.

4.1.1.2 This tool shall be interoperable with those SCCVI tools that are currently deployed in the "ENTERPRISE" (for example. Harris STAT, ISS, Foundstone, Nessus).

4.1.1.3 The system shall accept input and deliver output via standard data formats like tab delimited, Comma Separated Variable (CSV), and Extensible Markup Language (XML).

4.1.1.4 The system shall provide the capability to connect to a SQL database using the Open Database Connectivity (ODBC) standard.

4.1.1.5 Must be able to store and retrieve data from a SQL compatible database.

4.1.1.6 The system shall accept configuration and vulnerability-related remediation requirements provided by DoD expressed in OVAL eXtensible Markup Language (XML) when available.

4.1.1.7 The SCRI Tool shall provide an automated network quarantine capability. The solution shall provide the ability to detect devices as they attempt to connect to the network and ensure that the devices possess a secure configuration. If the device does not possess a secure configuration the solution will be able to isolate the device from the network until remediation occurs to bring the device into compliance.

4.1.1.8 The quarantine capability shall be an optional component of the solution provided allowing the SA to determine its applicability in a given environment.

4.1.1.9 The quarantine solution offered shall be interoperable with the SCRI Tool. Interoperability with the SCCVI tool, currently eEYE Retina, is desirable.

Deliverable: The SCRI Tool shall provide an automated network quarantine capability within six (6) months of award.

4.1.2 REMEDIATION REQUIREMENTS

4.1.2.1 The system shall provide the capability to perform policy based remediation. For example, create a remediation policy based on IAVMs, CVE, operating system type, or STIG compliance.

4.1.2.2 The system shall provide System Administrators (SAs) with the ability to conduct or schedule the remediation of known vulnerabilities at designated times.

4.1.2.3 The system shall permit SAs to select designated vulnerabilities to be repaired.

4.1.2.4 The system shall permit SAs to remediate based on grouping by domains, subnets, networks, IP address, system type, or class (e.g. server, workstation).

4.1.2.5 The system shall permit SAs to customize remediation signatures to enforce local policies/situations.

4.1.2.6 The system shall permit SAs to override specific vulnerability remedies via a capability that can be defined in the hierarchical remediation policy.

4.1.2.7 The system shall permit resume/recovery for interruptions during the remediation process.

4.1.2.8 The system shall provide confirmation of all fixes applied either independently or via rescan.

4.1.2.9 The system shall provide the capability to stop, start, or disable remediation services from the management console and be able to uncover the state of remediation services across the enterprise, and change start-up types.

4.1.2.10 The system shall provide controlled access to assets.

4.1.3 Selective Remediation Requirements

4.1.3.1 The contractor shall ensure that the tool has the capability to distribute a specified patch to a single system.

4.1.3.2 The contractor shall ensure that the tool has the capability to distribute a specified patch to multiple systems.

4.1.3.3 The contractor shall ensure that the tool has the capability to distribute a specified patch to a predefined group of systems.

4.1.3.4 The contractor shall ensure that the tool has the capability to distribute multiple patches to a single system.

4.1.3.5 The contractor shall ensure that the tool has the capability to distribute multiple patches to multiple systems.

4.1.3.6 The contractor shall ensure that the tool has the capability to distribute multiple patches to a predefined group of systems.

4.1.3.7 The contractor shall ensure that the tool has the capability to distribute multiple patches that are part of a predefined baseline.

4.1.3.8 The contractor shall ensure that the tool has the capability to schedule the distribution of a specified patch to a system.

4.1.3.9 The contractor shall ensure that the tool has the capability to schedule the distribution of a specified patch to multiple systems.

4.1.3.10 The contractor shall ensure that the tool has the capability to schedule a distribution of a predefined group of patches to a system.

4.1.3.11 The contractor shall ensure that the tool has the capability to schedule a distribution of a specified patch to multiple systems.

4.1.3.12 The contractor shall ensure that the tool has the capability to verify patch distribution was successful.

4.1.3.13 The contractor shall ensure that the tool has the capability to identify when patch installation has failed.

4.1.3.14 The contractor shall ensure that the tool has the capability to define a patch baseline for a system based on platform type

4.1.3.15 The contractor shall ensure that the tool has the capability to resume patching after interruption.

4.1.3.16 The contractor shall ensure that the tool has the capability to resume patch installation at the point at which interruption occurred.

4.1.3.17 The contractor shall ensure that the tool has the capability to rollback patches and return system to previous configuration.

4.1.3.18 The contractor shall ensure that the tool has the capability to determine patch dependency based on platform type.

4.1.3.19 The contractor shall ensure that the tool has the capability to use patch dependency.

4.1.3.20 The contractor shall ensure that the tool has the capability to flash bios versions and configurations.

4.1.3.21 The contractor should ensure that the tool has the capability to search and remove unauthorized software (e.g. Kazaa) as defined by the DoD.

4.1.3.22 The contractor shall ensure that the tool has the capability to support very low-bandwidth connections such as dial-up, as well as wireless, frame relays and satellite connections with minimal or no manual support required.

4.2 SCRI Instructions and Directives

The contractor shall comply with the appropriate DISA and DoD-approved architectures, programs, standards and guidelines, such as:

- DoD Directive 8500.1, Information Assurance
- DoD Instruction 8500.2, Information Assurance Implementation
- Global Information Grid (GIG) IA Technical Framework
- Defense Information Infrastructure (DII) Strategic Technical Guidance (STG)
- Common Operating Environment (COE)
- DII Standard Operating Environment (SOE)
- DISA Security Technical Implementation Guides (STIGs)
- National Security Agency (NSA) Security Guides
- Defense Information Systems Network (DISN)
- DoD Directive O-8530.1
- DoD Instruction O-8530.2 CND
- NSTISSP-11 policy
- NIST Spec Pub 800-23
- DoD Instruction 5200.40 DoD Information Technology Security Certification and Accreditation Process (DITSCAP)
- CJCSI 6510.01C, Information Assurance and Computer Network Defense
- CJCSM 6510.01, Defense-In-Depth: Information Assurance (IA) and Computer Network Defense (CND)
- DDOD 5200.1-R and the DOD 5220.22-M for handling classified material and producing deliverables.
- DISA Instruction 630-230-19.
- DISAI 210-20-2, Preparation and Processing of Data Collection and Analysis (DCA) Numbered Publications.
- NIST FIPS 140-2
- DoD 5000.1 (Defense Acquisition System, May 12, 2003)
- DoD 5000.2 (Operations of the Defense Acquisition System, May 12, 2003)

5.0 Scope

The Government requires a capability that will automate the remediation of vulnerabilities based on the DoD instructions. Examples of instructions/, guides include the DISA Security Technical Implementation Guide (STIG's), National Security Agency (NSA) System and Network Attack Center (SNAC). This ability must be selective in nature. Selective remediation means to perform remediation on a group of network assets or on a single network asset. This shall also include remediation of a single vulnerability or a group of vulnerabilities.

The CVE dictionary of named vulnerabilities is readily available on the public cve.mitre.org web site. One hundred and three contractors have declared that 167 products are or are being made CVE-compatible. In addition, in October 2003, NIST issued a Special Publication, SP 800-36 (Guide to Selecting Information Security Products), available at:
http://csrc.nist.gov/publications/nistpubs/800-36/NIST-SP800-36.pdf
The guide specifically recommends that "Whenever applicable, the tool should report the CVE number for each identified vulnerability."

The Government will have the option to test the contractor’s submitted products for the IA vulnerability SCRI Tool capability. This test, if conducted, will evaluate the tool's remediation of vulnerabilities using CVE numbers as well as all other requirements stated within this SOW.

This lab test shall be conducted as follows:

- Week 1 Security Test – SCRI submissions tested for STIG compliance. All proposals with no category one (I) findings will proceed to week 2 and 3.
- Week 2 and 3 Functionality Test – the SCRI submissions will be tested in accordance with the Measures of Merit.

5.1 SCRI Tool Interoperability Requirements (also refer to above Section 4.1.1 Interoperability Requirements)

The SCRI tool shall provide an interface to import data from the SCCVI (compliance) tool I-ASSURE Contract (IA 232) and shall provide interfaces to import data from service-level “ENTERPRISE” security assessment tools/systems currently in-use to maximum possible extent (e.g. Harris STAT, ISS, Foundstone, Nessus). The SCRI Tool must be able to remediate vulnerabilities reported by the SCCVI tool(s) in an automated fashion without manually reentering data. The SCRI Tool must provide a Graphical User Interface to guide the operator through the process of importing/reading the vulnerability data from the SCCVI tool. The product contractor shall provide a Vendor Integrity Statement (VIS) attesting that their proposed SCRI Tool is interoperable with service-level ENTERPRISE security assessment tools/systems in-use within the "ENTERPRISE". The product contractor shall not only provide the VIS but also provide a "technical overview" on how their product interoperates with the SCCVI tools and shall provide description of all necessary reconfiguration of the SCRI tool to support other service-level security assessment tools/systems interfaces. Having a structured program/process that can prove your product is "certified" as being interoperable with any/all SCCVI tools operational within the "ENTERPRISE” is desired.

The onus will be placed on the Government to provide as GFE to the offeror’s all service-level “ENTERPRISE” security assessment tools/systems are operational within the "ENTERPRISE".

The interoperability requirements are as follows:

(1) To import and aggregate data from the "ENTERPRISE's" SCCVI Tools: Structured Data Exchange and Unstructured Data Exchange.

(2) Seamless Sharing of Data: automated sharing of data amongst systems based on a common exchange model.

(3) Seamless Sharing of Information: universal interpretation of information through data processing.

6.0 Specific Tasks

Specific services addressed in this SOW are:

- Task Area 1 – Policy, Planning, Process, Program and Project Management Support
- Task Area 2 – Certification and Accreditation, Standards, Architecture, Engineering, and Integration Support
- Task Area 3 – SCRI Tool Solution Installation/Operations
- Task Area 4 – Education, Training and Awareness, Information Assurance (IA) Technical Support, and Contractor Priced Options

The government reserves the right to make multiple awards for this effort. Also, the offeror is only allowed to bid one solution for this effort.

6.1 Task 1 - Policy, Planning, Process, Program and Project Management Support

6.1.1 Subtask 1 - Support of both 120 Day Rapid Deployment and Lifetime of Contract

The contractor shall provide all software and hardware documentation/media to the Government to support the 120 day rapid deployment in Section 9.2.

Deliverable: 1. Software, Hardware, documentation/media due five (5) working days after the award of the TO. This is for the 120 day rapid deployment.

2. Software upgrades/documentation/media required to sustain for the life of the contract.

6.1.2 Subtask 2 - TO Management

The contractor shall provide the technical (task order level) and functional activities at the contract level needed for the Program Management of this SOW. Include productivity and management methods such as Quality Assurance, Progress/Status reporting, and Program Reviews at the Contract and Task Order level. Provide the centralized administrative, clerical, documentation and related functions.

The contractor shall prepare a TO Management Plan describing the technical approach, organizational resources and management controls to be employed to meet the cost, performance and schedule requirements throughout TO execution. The contractor shall provide a Bi-Weekly Status Report (BWSR) monitoring the quality assurance, progress/status reporting, and program reviews applied to the TO (as appropriate to the specific nature of the SOW).

Deliverable: 1. Management Plan due five (5) working days after the award of the Task Order (TO).

2. BWSR due every two weeks beginning after contract award.

6.1.3 Subtask 3 - Technical Support

Technical Interchange Meeting. The contractor shall host a Technical Interchange Meeting (TIM) to ensure a common understanding between the contractor and the Government on the TO requirements. Additional TIMs shall be held if determined by the Government's Task Manager (TM) - location TBD. If an additional TIM is held then the TIM notes deliverable will be required.

Deliverable: 1. Technical Interchange Meeting to be conducted NLT five (5) days after contract award.

2. TIM notes in written format are due NLT five (5) working days after the meeting.

6.1.4 Subtask 4 – Progress Reviews (Monthly IPR) / Meetings

The contractor shall conduct a monthly formal In Progress Review (IPR). This effort will start on day 30 after contract award and monthly after that. For the monthly IPR, the contractor's Technical Task Leader (TTL) and appropriate members of its technical team will meet with the appointed Government TM, and his/her associated members in person at a designated location as determined by the Government.

The contractor shall conduct Progress Review Meetings as deemed necessary by the Government. For these meeting's the contractor's Technical Task Leader (TTL) and appropriate members of its technical team will meet with the appointed Government TM, and his/her associated members in person at a location to be determined by the Government or via teleconference or a combination of both. The purpose of these meetings will be to informally discuss progress, request assistance as required, and deal with issues raised during the execution of the task.

Deliverable: 1. Monthly In Progress Review.

2. Progress Review Meetings /Monthly In-Progress Review notes in written format due NLT five (5) working days after the briefing.

6.1.5 Subtask 5 – Duplication of Effort

Ensure that there is minimal duplication of effort in the execution of all work specified in this SOW. Build upon work previously accomplished by the Government, the contractor, or other contractors to the fullest extent practical.

6.1.6 Subtask 6 - Cooperation/Coordination with Other Contractors

There may be multiple contractors (i.e. from more than one contract vehicle and/or company) supporting DISA and "The ENTERPRISE" tasked to work on the same or related activities. The contractor shall work with these other contractors as required to accomplish Government requirements, goals, and objectives as efficiently and effectively as possible. This may include, but is not limited to sharing or coordinating information resulting from the work required by this SOW or previous Government efforts, and/or working as a team to perform tasks in concert.

6.1.7 Subtask 7 - Personnel Management

The contractor shall provide and manage a complete, comprehensive team of highly qualified personnel able to accomplish the tasks specified in this SOW. The contractor shall also provide percentages of the time that these individuals will be dedicated to those tasks specified in this SOW.

6.1.8 Subtask 8 – Enterprise License

The contractor shall provide an unlimited enterprise license for the life of the contract to include upgrades with at least a one (1) year maintenance plan that allows "The ENTERPRISE" unlimited distribution, copying, and use.

The contractor will be authorized in accordance with the Federal Acquisition Regulation (FAR) part 51 to order from Enterprise Software Agreements of the DoD Enterprise Software Initiative (ESI), following ordering procedures substantially the same as Defense FAR Supplement 208.74. However, the contractor shall use a source that provides the best value to the Government.

We would also like to obtain favorable discounted software prices and terms for *future* DoD Enterprise Software Agreements (ESA) for IA software under the DoD Enterprise Software Initiative (ESI), http://www.don-imit.navy.mil/esi compared to what is offered to non-DoD customers. Offerors are encouraged to propose separate discounts for additional types of IA software from proposed software OEMs. This is desired but not required. The DoD ESI Team would incorporate these discounts into future ESA if possible. Software OEMs proposed in the offeror's quote should agree, as part of the quote, to credit the dollar value of their products in any resulting delivery order for this effort toward discounts calculated for spot price reductions under future ESA negotiated under the DoD ESI."

6.2 Task 2 – Certification and Accreditation, Standards, Architecture, Engineering, and Integration Support

6.2.1 Subtask 1 – National Information Assurance Partnership (NIAP) Certification

The Contractor shall submit with their proposal proof of NIAP certification at a minimum of EAL 2 or a letter of intent to commit to the NIAP certification process. Within 5 days of contract award, the contractor must show proof of contract that they are seeking NIAP certification if they are not currently NIAP certified. After contract award the contractor must provide proof of contract seeking NIAP approval at EAL 3 attainable within 12 months. The contractor shall ensure that each major release of the software will sustain NIAP Certification.

Deliverable: 5 days after award the contractor must provide proof of contract seeking NIAP approval.

6.2.2 Subtask 2 – STIG Compliance

STIGs provide instructions on securing operations in a specific technical environment. For this effort the contractor shall ensure that the SCRI tool and all functionality adheres to the applicable DISA STIG. STIG's are available from http://csrc.nist.gov/pcig/cig.html.

The Security Compliance Test will serve as a threshold "go/no go" evaluation criteria for this solicitation. After this test is run, if the Government determines that an integrator/contractor solution has any category 1 failures then they will not move on to the functional test and therefore will be eliminated from contention for this solicitation. Only one chance at passing the STIG test will be given to any integrator.

If the situation arises in which all the offeror's **do not** pass the Security Compliance Test Phase (SRR test) having category 1 errors on their first attempt, the integrator/contractor then would be given at the time of notification of these findings 48 hours to fix them. If these findings are not resolved via a second SRR test then the contractor's submitted proposal will then be eliminated from contention for this solicitation.

Upon contract award, the contractor's product solution will be certified and accredited via the DITSCAP process. The appointed DAA will ensure all vulnerabilities on the product are fixed or risk mitigation performed before granting the ATO approval. The product must receive an ATO before it is placed on any DoD network. This process is the government's method of ensuring the solution is STIG compliant.

6.2.3 Subtask 3 – IA Vulnerability Schemes and Interoperability

The contractor shall incorporate all "ENTERPRISE" instruction numbering schemes. Examples of the required instructions include the DISA Security Technical Implementation Guide (STIGs), NSA SNAC.

The SCRI tool shall provide the ability to input data from the SCCVI tool (eEye Retina Suite) or an ODBC link. The SCRI Tool must further accept input and deliver output via standard data formats like tab delimited, XML, and/or Comma Separated Value (CSV). The contractor shall

incorporate configuration and vulnerability-related checking requirements provided by DoD expressed in OVAL XML. Being compatible with OVAL means that each tool should be compliant with the "OVAL interface." That interface is described on the OVAL website at this URL:
http://oval.mitre.org/oval/schema/#XML_format

There are XML descriptions (schema) for the OVAL language itself and three platforms currently: Microsoft Windows, Solaris, and Red Hat Linux. These descriptions comprise the OVAL interface. In addition, there are over 500 OVAL definitions for testing vulnerabilities, and a handful of definitions for testing configuration items. It's the interface that's critical for the acquisition.

Deliverable: 1. Contractor will provide OVAL XML interface within 12 months of contract award.

6.2.4 Subtask 4 – Hierarchal Architecture

The contractor shall ensure that its SCRI tool is deployable to all networks within the "ENTERPRISE" to enable IA vulnerability remediation. This tool shall have the capability to share the results of its IA vulnerability remediation with many report-generating systems. The current SCCVI tool is eEye Retina Suite.

The management console should be accessible and an authenticated SA should be able to control the tool and generate reports through a secure (DoD PKI enabled) Web-based interface.

The SCRI tool will have the ability to conduct remediation from inside and outside the enclave under both local and external control.

The contractor shall ensure that the tool can be utilized in an organization's top-level architecture as well as within smaller enclaves that may be protected by firewalls and other security devices that are part of the DoD defense-in-depth posture.

The contractor shall ensure that the tool has the capability to log onto the patch management system locally. The contractor shall ensure that the tool has the capability to remotely log onto the patch management system.

6.2.5 NIST Certified Cryptographic Module Validation Program Certification

All communications within this hierarchal architecture, internal and external, shall be encrypted in accordance with a NIST Certified Cryptographic Module Validation Program. The contractor shall ensure upon proposal submission, provide proof of NIST Certified Cryptographic Module Validation Program compliance.

6.3 Task 3 - SCRI Tool Solution Installation/Operation

The contractor shall ensure that the capability fully integrates IA vulnerability remediation. Emphasis should include the capability to employ these tools in all operating environments, such as specified in the COE.

6.3.1 Subtask 1 - Automated Vulnerability Remediation, Closed Network Support, and Reporting

The contractor shall ensure that SA's have the capability within the tool that automates the tasks of vulnerability remediation. Their tool shall also provide the SA with step-by-step instructions appropriate for the platform to facilitate ease of installation and configuration operations. In addition, adequate help facilities (help pages) should be embedded within the tool to provide vulnerability information concerning the tasks above and possible remediation techniques. The tools shall further have the ability to be configured to obtain remediation software (e.g. patches) from a trusted DoD web site.

The contractor shall ensure that the tool has the capability to perform selective remediation on all networked devices to include operating systems and applications. Network devices are defined as any device on any DOD owned or controlled information system network, to include but not limited to workstations, servers, routing devices (router, switch, firewall), networked peripherals (e.g., network printers) and guards. The device is considered a single node on a network, such that it has its own network identification (internet protocol (IP) and/or media access control (MAC) address). The proposed SCRI tool shall be able to remediate IA vulnerabilities to include but not limited to the following; MS Windows Operating Systems (all variants from MS 95 to current) Sun Solaris, MS Internet Explorer, Netscape, MS Outlook, MS Exchange, Internet Information Server (IIS), SQL Server, Windows Terminal Server, Linux, and Firewalls. The contractor shall ensure that the tool has the capability to set, patch and or package prioritization, allowing the DoD to set priorities on updates. The contractor shall ensure that the tool has demonstrated performance in false positive rate verifications.

The contractor shall provide updates to their SCRI tool to the government. The government provides updates to "The ENTERPRISE". If the government finds any failures of the SCRI tool the contractor will have 24 hours after notification to correct the failure or provide a plan to correct the failure with milestones to identify how long the corrective action will take. The contractor provided software shall have a verification method such as an approved digital signature for validation of authenticity.

The SCRI tool shall support closed networks i.e., both NIPRNet and SIPRNet without the requirement to interface with contractors or other entities outside the enclave.

The contractor shall ensure that the tool is coupled with a central reporting capability and provides an effective means to remediate IA vulnerabilities.

The contractor shall ensure that the tool has the capability to generate reports automatically via a secure web-based interface as well as be capable of building selectable reports. The contractor shall ensure that the tool includes a report capability that will only be available to authenticated users from any machine with a DoD PKI enabled approved secure web based interface. The contractor shall ensure that the tool includes differential reporting capabilities based on a host, scalable group of hosts, or vulnerability with customizable reports. The tool shall provide the capability to create reports with the following criteria; DoD IAVM numbers, CVE numbers, CC, S/A, OVAL numbering schemes, the identity of the vulnerable systems, and the results of the remediation efforts. The tool shall provide both local and remote reporting securely using DoD certified encryption modules.

6.3.2 Subtask 2 - Field Proven Tools

The contractor shall ensure that the tool works in deployable, tactical, and isolated units (low BANDWIDTH/austere remote theater environments). Tool should have the capability to throttle back on bandwidth if needed to perform task.

6.3.3 Subtask 3 – Minimal impact on Normal Operations

The contractor shall ensure that the tool is able to run during normal operating hours with minimal impact on the user's mission. This tool must be capable of scheduling remediation activities at any time. Contractor shall ensure the tool is minimally disruptive to the operational environment.

6.3.4 Subtask 4 - Accountability and Enforcement

6.3.4.1 The contractor shall ensure that the SCRI tool allows for accountability of all remediation actions conducted. At a minimum the following audit trail information is required to establish accountability of remediation actions:

- Date remediation was performed
- The version of the product used for remediation
- The version of the product that was remediated (example OS, applications)
- Administrator who performed remediation operation
- Pass/Fail of remediation
- IP address, system/network name, and (where possible) MAC address of the system remediated.

6.3.4.2 The contractor shall ensure that the tool has the capability to create administrative accounts that are used by the patch management system.

6.3.4.3 The contractor shall ensure that the tool has the capability to grant permissions for the degree of access to the patch management system.

6.3.4.4 The contractor shall ensure that the tool has the capability to remove permissions for the degree of access to the patch management system.

6.3.4.5 The contractor shall ensure that the tool has the capability to delete administrative accounts that are used by the patch management system.

6.3.4.6 The contractor shall ensure that the tool has the capability to create administrative groups that are utilized by the patch management system.

6.3.4.7 The contractor shall ensure that the tool has the capability to delete administrative groups that are used by the patch management system.

6.3.4.8 The contractor shall ensure that the tool has the capability to grant permissions to administrative groups that are used by the patch management system.

6.3.4.9 The contractor shall ensure that the tool has the capability to log changes to administrator permissions.

6.3.4.10 The contractor shall ensure that the tool has the capability to log changes to administrative group permissions.

6.3.4.11 The contractor shall ensure that the tool has the capability to notify of inactive patch management administrators based on predefined time limit.

6.3.4.12 The contractor shall ensure that the tool has the capability to provide detailed audit log capability.

6.3.4.13 The contractor shall ensure that the tool has the capability to tailor auditing.

6.4 Task 4 - Education, Training and Awareness, IA Technical Support, and Contractor Priced Options

6.4.1 Subtask 1 – Virtual On-Demand Training for SCRI tool

Past implementation experience in deploying IA tools within "The ENTERPRISE" has proven that without training, a large percentage of those tools remain on the shelf and will not get used. Lack of training has adversely affected operational performance through misuse or the capabilities of the tools are under-utilized, resulting in a poor return on investment. With the expanding capabilities IA tools and their associated potential devastation to operational networks, it is imperative that administrators are trained to utilize IA tools on a virtualized network before installing on their real networks.

To provide comprehensive training for this IA specific training tool, the contractor shall provide a capability to leverage advancements in interactive training environments, to provide a virtual and interactive, on demand IA training program. This capability shall allow for distributed, worldwide accessibility from the users perspective from their duty location; and permit the distribution of this virtualized training to remote or austere locations.

Students shall be able to login, via a secured web interface, to a virtual interactive classroom that offers a variety of teaching tools, e.g. streaming audio, streaming video, interactive chat, web boards or virtual servers. The virtual training environment shall focus on tool utilization and implementation, and shall be capable of student evaluation or testing to ensure adequate skills are obtained. The virtual training environment will allow the student to return to an archived point in a previously started training session.

The use of the IA tool in the virtualized environment shall cause no impact to the operational network or services, nor require operational assets to be accessible to the IA tools for operation.

The contractor shall be responsible to update the online training within 5 days of every major software upgrade; with incremental changes as determined during a monthly review of the online training to reduce the lag time that now occurs in updating or improving individual technical skills. The contractor shall maintain this training for the lifetime of the contract.

The online training package shall be Section 508 compliant.

Deliverable: 1. Online training package and certification test within 30 days of TO award.

2. Update the online training within 5 days of every major software upgrade with incremental changes as determined.

6.4.2 Subtask 2 - Classroom Training Support.

The contractor shall provide instructors who have expert knowledge of and experience with the SCRI tool. The contractor is to provide SCRI tool classroom training to various "ENTERPRISE" (CONUS/OCONUS) locations.
The classroom training is intended to be given to the core team from Combatant Commands, Services and Agencies-

CONUS – Twenty Classes

OCONUS – Pacific Area of Responsibility (AOR) – Five Classes
Europe AOR - Five Classes
Southwest Asia (SWA) AOR – Five Classes

The contractor shall provide a hands-on training environment that will accommodate up to 875 students in the base year of the contract, up to 25 students per class. The training environment will consist of a training classroom, manuals, hardware (student workstations and laboratory environment), and software to support 25 students. Following completion of the classroom training the student will be tested to ensure adequate understanding of the SCRI tool is obtained. The contractor shall maintain a schedule of courses, which will be approved by the Government. The contractor shall ensure the continuity of instructors for the duration of the task. Considered key personnel, instructors shall be approved by the Government prior to teaching and must maintain an above average rating on student course evaluations. The instructor shall submit an After Action Report within five (5) working days after the end of each course. Upon approval of the Government, the contractor shall support update of courses based on after action reports, student evaluations and other relevant feedback. Training will be maintained for the life of the contract.

The contractor shall be responsible to update the classroom training within 5 days of every major software upgrade; with incremental changes as determined during a monthly review of the online training to reduce the lag time that now occurs in updating or improving individual technical skills.

The contractor shall be responsible for generating DISA approved course materials (to become the Intellectual Property of DISA), making sufficient copies of the student materials, shipping them to the training sites, and administering a DISA approved Trainer Certification test.

Deliverable: 1. Course Materials (Screen shots, Student handbook, Critique, etc.), Trainer Certification test submitted for approval by day 20 after award. After Action Reports are due 5 days after classroom training has been completed.

2. Update the classroom training within 5 days of every major software upgrade; with incremental changes as determined.

6.4.3 Subtask 4 - Technical Support for SCRI Tool

The capability shall be available to the Government at Support levels 1, 2, and 3 which is provided 24x7x365 days a year. This should include but not limited to; maintaining a frequently asked questions (FAQ) online database and weekly reports.

Technical Support.

- Level 1 support will answer technology-related questions and participate in solving technical issues. They will also help with hardware and software installation issues and keeping records of technical issues that are called into the level 1 help desk. They will contact Level 2 support for issues that cannot be resolved.

- Level 2 supports will consist of advanced technical issues from installs, upgrades and hardware failure. This level will organize and maintain records of trouble calls in a database to be used in doing comparisons and performing analysis of the data. This information will also be made available, on a weekly basis, through FAQ's information specific to DOD.

- Level 3 support identify, isolate, and resolve software anomalies.

Deliverable: Contractor shall provide help desk support Starting on Day 5 of award.

6.4.4 Subtask 5 - Support for SCRI Tool During 120 Day Deployment Plan (See section 9)

The contractor shall provide on-site technical support for a 120-Day Deployment Plan as requested by the Government. This at a minimum will include 240 hours of onsite technical support.

Deliverable: 240 hours of onsite technical support.

6.4.5 Subtask 6 – Contractor Price Options

6.4.5.1 Hardware Price Options

The contractor shall provide a hardware solution for "The ENTERPRISE" license. The hardware specification is to include cost estimates per solution.

6.4.5.2 Additional Contractor Training Option

The contractor shall provide a cost estimate to satisfy additional classroom training for 125 seats. The training shall be conducted throughout "The ENTERPRISE". Please break down the training options in the following manner:

OPTION 1:

CONUS – 50 seats

OCONUS – Pacific Area of Responsibility (AOR) – 25 seats
Europe AOR -25 seats
Southwest Asia (SWA) AOR – 25 seats

OPTION 2:

CONUS – 65 seats

OCONUS – Pacific Area of Responsibility (AOR) – 20 seats
Europe AOR -20 seats
Southwest Asia (SWA) AOR – 20 seats

The contractor shall also provide the Government with a cost estimate per seat in both the CONUS and OCONUS areas. Please break out per Combatant Command and regional location. Price discounts will be provided to the Government based on the number of seats/personnel to be trained.

6.4.5.3 Deployable SCRI Training Support Option.

The contractor shall provide a cost estimate for further mobile training kits that are completely self-contained, fully functional and operational and that mirrors the above proposed classroom training to accommodate at a minimum 10 students. This kit shall include detailed, step-by-step instructions on how to set up the classroom as well as how to tear it down. Please price out on a per kit basis. The Government encourages favorable price discounts for bulk buys of these kits.

7. Place of Performance

The contractor's team shall perform the majority of the SOW work at their facility, with a contingent located at but not limited to the various "ENTERPRISE" locations. Contractor personnel shall also perform Temporary Duty (TDY) to DISA customer locations, as listed, but not limited to, in paragraph 8.0 below. A contractor representative, considered a subject matter expert (SME), shall be located at a CONUS location to be determined by the government.

Deliverable: Contractor shall provide a SME on day 5 after contract award.

8. Travel

The contractor shall be required to travel to support this contract. Local travel within the National Capital Region and to Letterkenny Army Depot (DISA Field Security Office (FSO)), Chambersburg, PA is required and authorized. Travel will be required throughout “The ENTERPRISE”. The Government will review for approval all travel orders under this SOW prior to the travel taken place. The contractor shall provide an estimate of required travel to support this effort.

9. Period of Performance

The Task Order awarded through the I-ASSURE vehicle will consist of a one (1) twelve-month base year with four (4) one-year option periods. The option periods are to be exercised upon a favorable review of the contractor's performance, validation of continued need and a review of negotiated prices compared to recently awarded contracts similar in scope and nature to ensure prices are neither too high or too low.

9.1 Pre Award

The government reserves the right to test the SCRI tool solution before contract award. This test may be done in multiple locations and/or in multiple test beds. If the government elects to test the tool solutions the contractor shall be required to provide a fully functional SCRI tool that will be STIG compliant. If the proposed tool requires specialized hardware installation, the contractor will provide and configure the hardware component. The Government will determine the test location(s).

9.2 Post Award

120-Day Rapid Deployment

- Day 2 Conduct informal TIM
- Day 5 Software; Hardware to support 3 tool suites for each of the 5 test locations; 2 tool suites for SIPRNet; 4 tool suites for DISA FSO certification and accreditation (C & A), help desk support, SME and Documentation delivery. This requires a total of 21 total tool suites
- Day 5 (NLT) Conduct TIM
- Day 5-35 Security Testing & IATO
- Day 30 IPR
- Day 40 Begin Phase I
    - One Combatant Command

- Day 60 Phase I IPR
- Day 70 Phase II
  - One site per Service
- Day 90 IPR
- Day 120 IPR
- Day 120 Full Operational Capability (FOC)

Life of the Contract

- Program reviews as required after the 120 rapid deployment

Deliverable: Hardware to support 3 tool suites for each of the 5 test locations, 2 tool suites for SIPRNet, 4 tool suites for DISA FSO certification and accreditation (C & A) This requires a total of 21 total tool suites. The contractor shall deliver on day 5 after contract award.

10. **Delivery Schedule**

SOW Task #	Deliverable Title	Format	Due Date	Distribution	Frequency and Remarks
6.1.1	Software, hardware, help desk support, SME and documentation/ media Delivery		5 Working days after TO award		
6.1.2	Management Plan	Contractor Format	5 Working days after TO award		
6.1.2	Bi-Weekly Status Report	Contractor Format	Every two weeks beginning after contract award	Standard Distribution* ***Business Office	
6.1.3	Informal TIM	N/A	2 Working days after TO Award		
6.1.3	Technical Interchange Meeting	N/A	5 Calendar days after TO award		
6.1.3	TIM notes	Contractor Format	5 Working days after TIM		
6.1.4	Monthly In-Progress Review Progress Review Meetings	Contractor Format	30 Calendar days after TO award TBD		30 days after contract award monthly thereafter As deemed necessary by the Govt

6.1.4	Monthly In-Progress Review notes Progress Review Meeting notes	Contractor Format	5 Working days after Monthly In-Progress Review and Meetings		
6.2.1	Provide proof of seeking NIAP certification	Contractor Format	5 Calendar days after TO award		
6.2.3	OVAL XML Interface	XML format	365 Calendar days after TO award		
6.4.1	Virtual On-Demand Training Package/ Certification Package	Contractor Format	30 Calendar days after TO award		
6.4.1	Virtual On-Demand Training Package/ Certification Package	Contractor Format	5 Calendar days after S/W Updates		
6.4.2	Classroom training support	Contractor Format	20 Calendar days after TO award		
6.4.2	Classroom training support	Contractor Format	5 Calendar days after S/W Updates		
6.4.2	Classroom Course Materials	Contractor Format	20 Calendar days after TO award		
6.4.2	After Action Report	Contractor Format	5 Working days after class has been completed		
	On-site Tech	N/A	At		

6.4.4	Support - 240 hours		Government Request		

* Copies

- Hard copy (HC)
- Soft copy (SC) Soft copy for reports, minutes, white papers, etc., will be in MS Word, Office 2000 version. Soft copy for briefings will be in PowerPoint, Office 2000 version. Soft copy can be contained on CD-ROM, ZIP Drive, or Floppy as appropriate for size.
- Bound hard copy (BHC) - All functional and design documents must be spiral or notebook bound.

***1 copy of monthly status reports only to Business Office

Note 1: Cost and status reports are due 14 days after close of contractor's accounting period.

11. Security/Clearance Requirements

The following security requirements shall apply to this effort:

Secret - Access to Information/Personnel Security Clearances
TS/SCI - A contractor representative, considered a subject matter expert, shall be located at a CONUS location to be determined by the government.

Classified Information. All contractor personnel performing work under this effort shall have access to classified information at least up to and including SECRET. Therefore, all contractor personnel shall have a minimum of a SECRET security clearance. The Technical Task Leader (TTL) will require a Top Secret clearance to perform his/her duties on this TO.

Position Designation. The TTL must have a minimum clearance of Top Secret and a position sensitivity designation of Automated Data Processing (ADP)-I. All system and/or database administration, quality assurance/code reviewer, and technical team lead personnel must have a minimum clearance of Secret and a position sensitivity designation of ADP-I. The minimum investigation required is a Single Scope Background Investigation. All Editor/Analysts, Administrative Assistants, and developers not performing in roles listed above will have a minimum clearance of Secret and a position sensitivity designation of ADP-II. The minimum investigation required is a NACLC. All work performed by a developer holding a sensitivity designation of ADP-II must have their work reviewed by someone holding a sensitivity designation of ADP-I. No more than three developers can occupy ADP-II positions. All personnel performing on this contract will be U.S. citizens.

Obtaining Clearances. The contractor is responsible for obtaining personnel security clearances from the Defense Security Service (DSS). The contractor shall assure that individuals assigned to this contract will have completed the SF 86, Electronic Personnel Security Questionnaire (EPSQ) and then take the required action to submit the personnel security investigative (PSI) packet electronically to the Defense Security Service. The required investigation will be completed prior to the assignment of individuals to sensitive duties associated with their position. The contractor shall forward a Visit Authorization Letter (VAL) on all their employees to the TM.

ADP Determination. Upon submission of PSI packet to DSS, the contractor will provide a complete signed copy of the PSI packet (SF 86, Electronic Personnel Security Questionnaire; DD Form 1879, DOD Request for Personnel Security Investigation or National Agency Check (NAC) information; and the EPSQ Receipt System Results) to address listed in paragraph 10.3 above in order to obtain an ADP determination.

Interim Clearances. An interim clearance, at the contract-required level, and interim ADP, at the contract-required level, would suffice for the contractor employee to start work on the contract.

Contractor Generated Documents. Contractor personnel can generate or handle documents that contain FOUO information at both Government and contractor facilities. Contractor shall have access to, generate, and handle classified material only at Government facilities. All contractor deliverables shall be marked at a minimum FOUO, unless otherwise directed by the Government. The contractor shall comply with the provisions of the DOD 5200.1-R and the DOD 5220.22-M for handling classified material and producing deliverables. The contractor shall also comply with DISA Instruction 630-230-19.

Security Procedures. All contractor personnel working on or managing this effort shall strictly adhere to DISA and DOD security regulations and procedures. In addition, all contractor personnel shall comply with local security requirements as established by the facility being supported.

Sensitive Data Stored at Contractor Facilities. The contractor shall ensure that any sensitive information or code stored at contractor facilities is protected in compliance with Security Standard Operating Procedures.

12. Government-Furnished Equipment (GFE)/Government-Furnished Information (GFI)

GFE and contractor-acquired Government owned equipment may possibly be used for this Statement of Work (SOW) under this delivery order. Any hardware or software procured under DISA's approval for this contract shall remain property of the Government, and shall be returned to the Government as specified by the TM at the conclusion of the contract. The TM will provide a detailed list.

13. Other Pertinent Information or Special Considerations

The contractor must be able to implement current industry standard certified quality management processes (e.g. ISO 9001, Capability Maturity Model) to evaluate, measure, report, and improve remediation capabilities. The contract team shall provide the optimum mix of personnel of various labor categories and technical expertise to perform the tasks specified in this SOW in the technical environments specified in this SOW.

13.1 Possible follow-on work

The Government may continue much of the work specified in this Delivery Order (DO), past the performance period specified herein. Contractor support may be required.

13.2 Identification of Non-Disclosure Requirements

All contractor personnel working on this effort must execute nondisclosure agreements prior to commencement of their starting work on this effort.

13.3 Cooperation/Coordination with other Contractors

Because of the rapidly changing nature of information infrastructure threats, very open collaboration is essential for the DoD to act as a coordinated team in a timely manner. This team consists of military, government civilians, and contractors. Working under this SOW requires broad cooperation with multiple contractors (i.e., from more than one contract vehicle/company) working in the same or dispersed locations supporting DISA, DECCs, RNOSCs, RCERTs, Agency/Service CERTs, Combatant Commanders IA Teams, other Agencies and civilian organizations. The contractor shall work with these other contractors and organizations as required, accomplishing Government requirements, goals, and objectives as efficiently and effectively as possible. This cooperation may include but is not limited to sharing information such as white papers, sharing training efforts, exchanging tactics, tools, and/or procedures resulting from the work required by this SOW or other Government task efforts, and/or working as a team to perform analysis as well as technical tasks and contingency activities in concert. Any concerns about possible disclosure of company proprietary data should be brought to the TM.

13.4 Technology Refresh

The contractor shall continually assess their SCRI tool(s) for future expansion and remediation capabilities of acquisitions or emerging products. This Information shall be provided to the government during the monthly progress review briefings. These shall include, but are not limited to IPv6 support, host-based intrusion prevention, and operating system protection capabilities. Ensure tool is compatible or has the ability to be upgraded to run on future platforms.

13.5 Use of Consultants

Due to the unique nature of the work and "state-of-the-art" analysis, on occasion, DISA may find it necessary to call upon the expertise of technical experts from various and/or unique technology fields, academia, or non-governmental activities with special or critical knowledge that may contribute to the understanding, techniques or analysis that DISA may be required to perform. As directed by the TM, the contractor will be prepared to facilitate bringing this consultant expertise on to support above said activities whenever possible.

13.6 System Documentation

The Government shall have "Government purpose rights" which means the rights to use, modify, reproduce, release, perform, display, or disclose technical data within the Government without restriction, and release or disclose technical data outside the Government and authorize persons to whom release or disclosure has been made to use, modify, reproduce, release, perform, display, or disclose that data for United States government purposes.

a. Identification of Potential Conflicts of Interest (COI). At any point during the performance of the contract, if either the government or the contractor perceives a conflict of interest, they are required to inform the other party for resolution.

b. Identification of Non-Disclosure Requirements. All contractor personnel working on this effort must execute nondisclosure agreements prior to commencement of their starting work on this effort.

c. Packaging, Packing and Shipping Instructions. Contractor shall be responsible for shipping required equipment to government installation and testing sites.

d. Inspection and Acceptance Criteria. All technology deliverables shall comply with DoD Instruction 5200.40 DITSCAP or its successor document, and be accredited at highest level of the connection it supports. Documentation deliverables shall be grammatically correct and technically accurate. Inspection of deliverables shall be conducted at the government site. The TM will review all draft and final deliverables to ensure accuracy, functionality, completeness, professional quality, and overall compliance within the guidelines/requirements of the delivery order. Unless otherwise indicated, the government will require 20 workdays to review and comment on deliverables. If the deliverable does not meet the noted criteria, the Government in accordance with the Contract Data Requirements List (CDRL) will return it.

13.7 Rejection Procedures

A rejected deliverable will be handled in the following manner:

> After notification that the deliverable did not meet the acceptance criteria the contractor shall resubmit updated/corrected version 15 workdays after receipt of government comments. Upon re-submission by the contractor the Government will reapply the same acceptance criteria. If the deliverable does not meet the acceptance criteria a second time the government might consider the contractor as having deficient performance with respect to the subject task.

13.8 Exchange of Information With Other Organizations

This project could require contractor personnel to exchange classified information with representatives of:

OSD/NII, the Joint Staff, NSA, DIA, Combatant Commands, and the Services.

The contractor shall not distribute material or documents generated under this statement of work to anyone including contractor offices or personnel not directly involved on this project until written approval is received from DISA. The contractor shall deliver required work efforts in both draft and final versions according to schedule data. All final deliverables will be published under DISA cover unless directed otherwise by the Government. Final paper deliverables shall be printed on 8.5” by 11” paper, double-sided print in the numbers indicated. One (1) final paper deliverable shall remain unbound. Draft deliverables shall be delivered in double-sided print and remain unbound. The contractor shall also deliver one (1) copy of each deliverable on electronic media in Microsoft Word format. All delivered electronic media shall be free of malicious code (including but not limited to boot sector and Word Macro viruses). Unless specified, the maximum number of deliverables will be no more than five (5) copies. For deliverables relating to format DISA publications (i.e., instructions, standard operating procedures, supplements, circulars), the contractor shall use format provided in DISAI 210-20-2, Preparation and Processing of Data Collection and Analysis (DCA) Numbered Publications.

13.9 Purchase of Materials on Behalf of the Government

The contractor, at the direction of the Government, shall purchase materials (e.g., ADPE) that will be used in support of this Task Order. Any materials purchased on behalf of the Government will become the property of the Government.

13.10 Limit on Submission of Products

Each Integrator shall submit one and only one product for evaluation. Multiple products from the same Integrator will not be evaluated.

13.11 Multiple Awards

The Government reserves the right to award contracts to multiple Integrators.

14. Documentation of Past Performance – The contractor shall demonstrate acceptable past performance within the areas listed in the subtasks listed below:

14.1 – Subtask 1 – Documentation of Commitment to Customer Satisfaction on Past Projects

The contractor shall demonstrate commitment to customer satisfaction including strong Project Management, (i.e. meeting cost, schedule, and performance targets, and mature software and systems engineering/integration methods and processes for comparably sized programs).

14.2 – Subtask 2 – Documentation of Demonstrated Expertise in Partnering

The contractor shall demonstrate expertise in Contractor/Contractor and Contractor/Government partnering or teaming environments to include strong subcontractor management (if proposal includes subcontracting) and the ability to work cooperatively with other contractors to ensure that the Government customer's overall cost, schedule, and performance (customer satisfaction and quality of service/product/solution) targets are met.

14.3 – Subtask 3 – Documentation of Experience with DOD IA Security Methodologies

The contractor shall demonstrate experience with appropriate DISA and DoD-approved architectures, programs, standards and guidelines related to IA security methodologies.

14.4 – Subtask 4 – Documentation of Experience in Information Assurance

The contractor shall demonstrate depth and breadth of experience and technical competence in Information Assurance areas to include: network security and certification, Information Assurance Vulnerability Management (IAVM), and computer operating systems.

14.5 - Subtask 5 – Documentation of Experience in Product Training

The contractor shall demonstrate experience with providing top-level training classes of their product both in a classroom and virtual On-demand settings

14.6 – Subtask 6 – Documentation of Experience in Help Desk Functionality and Customer Support Operations

The contractor shall demonstrate experience with providing timely and responsive Help Desk and customer support operations at all levels of support. The contractor shall also demonstrate their ability to provide the requisite level of technical expertise at each help desk stage (levels 1, 2, and 3) to ensure customer satisfaction.

15. Section 508 Accessibility Standards. The following Section 508 Accessibility Standard(s) (Technical Standards and Functional Performance Criteria) are applicable (if box is checked) to this acquisition.

Technical Standards

☒ 1194.21 - Software Applications and Operating Systems
☒ 1194.22 - Web Based Intranet and Internet Information and Applications
☒ 1194.23 - Telecommunications Products
☒ 1194.24 - Video and Multimedia Products
☐ 1194.25 - Self-Contained, Closed Products
☒ 1194.26 - Desktop and Portable Computers
☐ 1194.41 - Information, Documentation and Support

The Technical Standards above facilitate the assurance that the maximum technical standards are provided to the Offerors. Functional Performance Criteria is the minimally acceptable standards to ensure Section 508 compliance. This block is checked to ensure that the minimally acceptable electronic and information technology (E&IT) products are proposed.

Functional Performance Criteria

☒ *1194.31 - Functional Performance Criteria*

16. Descriptions

Application.

1. Reference is often made to an application as being either of the computational type, wherein arithmetic computations predominate, or of the data processing type, wherein data handling operations predominate.

2. In the intelligence context, the direct extraction and tailoring of information from an existing foundation of intelligence and near real time reporting. It is focused on and meets specific, narrow requirements, normally on demand.

Architecture. The configuration of any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information; includes computers, ancillary equipment, and services, including support services and related resources.

Assurance. A measure of confidence that the security features and architecture of an AIS accurately mediate and enforce the security policy. If the security features of an information system (IS) are relied on to protect classified or sensitive unclassified information and restrict user access, the features must be tested to ensure that the security policy is enforced and may not be circumvented during IS operation.

Automated Vulnerability Remediation. The ability for an application to automatically remediate vulnerabilities based on operator input. The operator has the ability to selectively remediate (or not remediate) one, some, or all vulnerabilities based upon network architecture, legacy or program managed systems, bandwidth, operational constraints, and other interrelated factors that may have a direct or implied impact on an organization's mission.

Common Criteria. The International Common Criteria for Information Technology Security Evaluation (CC) defines general concepts and principles of information technology (IT) security evaluation and presents a general model of evaluation. It presents constructs for expressing IT security objectives, for selecting and defining IT security requirements, and for writing high-level specifications for products and systems.

Common Operating Environment. The collection of standards, specifications, and guidelines, architecture definitions, software infrastructures, reusable components, application programming interfaces (APIs), (LB) runtime environment definitions, reference implementations, and methodologies, that establishes an environment on which a system can be built. The COE is the vehicle that assures interoperability through a reference implementation that provides identical implementation of common functions. It is important to realize that the COE is both a standard and an actual product.

Common Vulnerability Exposure - A list of standardized names for vulnerabilities and other information security exposures - CVE aims to standardize the names for all publicly known vulnerabilities and security exposures.

Computer Emergency Response Team(s) (CERT). CERTs are teams composed of personnel with technical expertise and organic equipment that may deploy to assist remote sites in the restoration of computer services. Services have formed CERTs as an operational organization for rapid response to both deployed and installation based Service forces. Note: Some teams may be referred to as Computer Security Incident Response Team(s) (CSIRT) or computer incident response team(s) (CIRT).

Computer Network Defense (CND). Actions taken to protect, monitor, analyze, detect and respond to unauthorized activity within DOD information systems and computer networks. NOTE: The unauthorized activity may include disruption, denial, degradation, destruction, exploitation, or access to computer networks, information systems or their contents, or theft of information. CND protection activity employs information assurance protection activity and includes deliberate actions taken to modify an assurance configuration or condition in response to a CND alert or threat information. Monitoring, analysis, detection activities, including trend and pattern analysis, are performed by multiple disciplines within the Department of Defense, e.g., network operations, CND Services, intelligence, counterintelligence, and law enforcement. CND response can include recommendations or actions by network operations (including information assurance), restoration priorities, law enforcement, military forces and other US Government agencies.

Data. Representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or automatic means. Any representations such as characters or analog quantities to which meaning is or might be assigned.

Defense Information Infrastructure (DII). The shared or interconnected system of computers, communications, data applications, security, people, training, and other support structures serving DoD local, national, and worldwide information needs. The Defense Information Infrastructure connects DD mission support, command and control, and intelligence computers through voice, telecommunications, imagery, video, and multimedia services. It provides information processing and services to subscribers over the Defense Information Systems Network and includes command and control, tactical, intelligence, and commercial communications systems used to transmit DoD information.

DISA Regional CERTs. CONUS-RCERT at Scott AFB (IL), EUR-CERT at Stuttgart (Germany), PAC-CERT at Wheeler AAF (HI), and Central-CERT at Manama (Bahrain).

Defense Information Systems Network (DISN). A sub-element of the Global Information Grid (GIG), the DISN is the DOD's consolidated worldwide ENTERPRISE level telecommunications infrastructure that provides the end-to-end information transfer network for supporting military operations. It is transparent to its users, facilitates the management of information resources, and is responsive to national security and defense needs under all conditions in the most efficient manner.

DOD CERT. DoD Computer Emergency Response Team, located at DISA Headquarters in Arlington, VA.

DoD Information Technology Security Certification and Accreditation Process (DITSCAP). The standard DoD process for identifying information security requirements, providing security solutions, and managing information system security activities.

"The ENTERPRISE". Department of Defense, Coast Guard, Intelligence Community, National Guard and the Reserves comprise the enterprise

eXtensible Markup Language (XML) - XML is the Extensible Markup Language. It is designed to improve the functionality of the Web by providing more flexible and adaptable information identification. It is called extensible because it is not a fixed format like HTML (a single, predefined markup language). Instead, XML is actually a `meta-language' (a language for describing other languages) that lets you design your own customized markup languages for limitless different types of documents. XML can do this because it's written in SGML, the international standard meta-language for text markup systems (ISO 8879).

Full Operational Control (FOC) - FOC means that the solution will be fully operational and available for the Enterprise's use.

IA vulnerability. DoD CERT Information Assurance Vulnerability Alerts (IAVMs) Information Assurance Vulnerability Bulletins and Information Assurance Vulnerability Technical Advisories (IAVB/TAs) security patches.

Information. 1. Facts, data, or instructions in any medium or form. 2. The meaning that a human assigns to data by means of the known conventions used in their representation.

Information Assurance (IA). Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. Note: This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Information Assurance Watch Team. IA Watch Team guides customers to several on-line INFOSEC resources, including, an anonymous FTP site for alerts and tools and DISA web pages to aide in the dissemination of vital INFOSEC information.

Information System (IS). The entire infrastructure, organization, personnel, and components for the collection, processing, storage, transmission, display, dissemination, and disposition of information.

Interoperability: The ability of two or more systems or components to exchange information and to use the information that has been exchanged

Malicious Code. Viruses, Trojan Horses, Worms, and Backdoors.

National Information Assurance Partnership (NIAP). A collaboration between the National Institute of Standards and Technology (NIST) and NSA to meet the security testing needs of both information technology producers and users. The program is intended to foster the availability of objective measures and test methods for evaluating the quality of IT security products and provide a sound and reliable basis for the evaluation, comparison and selection of security products.

Network Device. Network devices are defined as any device on any DOD owned or controlled information system network, to include but not limited to workstations, servers, routing devices (router, switch, firewall), networked peripherals (e.g., network printers) and guards. The device is considered a single node on a network, such that it has its own network identification (internet protocol (IP) and/or media access control address).

Non-secure Internet Protocol Routing Network (NIPRNET). Non-classified Internet Protocol Routed Network.

Open Vulnerability Assessment Language (OVAL) - OVAL is the common language used by security experts to discuss technical details about how to check for the presence of vulnerability on a computer system.

Secondary CERTs. DISA Regional CERTs, Service CERTs and Agency CERTs

SECRET Internet Protocol Router Network (SIPRNET). Worldwide SECRET level packet switch network that uses high-speed Internet protocol routers and high-capacity Defense Information Systems Network circuitry.

Secure Configuration Remediation Initiative (SCRI). The comprehensive distribution process for notifying Combatant Commanders, Services and Agencies (CC/S/A) about vulnerability alerts and countermeasures information. The IA vulnerability Program requires CC/S/A receipt acknowledgment and provides specific time parameters for implementing appropriate countermeasures depending on the criticality of the vulnerability.

Selective Remediation. The means to perform remediation on a group of network assets or on a single network asset. This shall also include remediation of a single vulnerability or a group of vulnerabilities.

Service CERTs. Army CERT (ACERT) at Ft. Belvoir, VA, Air Force CERT (AFCERT) at Lackland Air Force Base, TX, Navy CERT (NAVCIRT) at Norfolk, VA, Coast Guard CERT (CGCERT) at Alexandria, VA and Marine CERT (MARCERT) at Quantico, VA.

System Administrator (SA). Individual responsible for the installation and maintenance of an information system, providing effective information system utilization, adequate security parameters, and sound implementation of established INFOSEC policy and procedures.

Technical Support.

- Level 1 support will answer technology-related questions and participate in solving technical issues. They will also help with hardware and software installation issues and keeping records of technical issues that are called into the level 1 help desk. They will contact Level 2 support for issues that cannot be resolved.

- Level 2 supports will consist of advanced technical issues from installs, upgrades and hardware failure. This level will organize and maintain records of trouble calls in a database to be used in doing comparisons and performing analysis of the data. They will also contact the PMO and Level 3 for issues that cannot be resolved.

- Level 3 supports will be the contractor of the product to be supported. They will work with both Levels of support and the PMO, getting any and all problems resolved in a timely manner.

Threat. Any circumstance or event with the potential to harm an information system through unauthorized access, destruction, disclosure, modification of data, and/or denial of service.

Virtual Private Network (VPN). Protected information system link utilizing tunneling, security controls (see information assurance), and end-point address translation giving the user the impression a dedicated line exists between nodes.

Virus. A self-reproducing program or code that may attach itself to other programs and files.

Vulnerability. A weakness in a system allowing unauthorized access.

Vulnerability Assessment. Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

Worm. A self-replicating program or code that spreads without human intervention.