ORDER FOR SUPPLIES OR SERVICES

PAGE 1 OF 41

1. CONTRACT/PURCH. ORDER/ AGREEMENT NO. DCA200-00-D-5021	2. DELIVERY ORDER/ CALL NO. 0021	3. DATE OF ORDER/CALL 2004 Jun 03	4. REQ./ PURCH. REQUEST NO. DGEMZ49877	5. PRIORITY

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
☒ 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. REF:

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 $4,363,728.94

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

31. PAYMENT
□ COMPLETE
□ PARTIAL
□ FINAL

32. PAID BY

33. AMOUNT VERIFIED CORRECT FOR

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	$3,657,680.55	$3,657,680.55

Information Assurance Support Services
FFP CLIN
DoD-Wide Enterprise Licenses for an automated Information Assurance Vulnerability Management (IAVM) Compliance Tool as in accordance with SOW dated 29 Apr 04 which is an attachment to this order. Period of performance is from 03 Jun 04 thru 02 Jun 05 as in accordance with DigitalNet proposal dated 30 Apr 04 which is incorporated by reference.

This FFP line item includes:

Enterprise Licenses –	$3,095,242.50
Training Support -	$ 38,011.75
Technical Support -	$ 352,966.25
Help Desk Option	$ 61,904.85
Training Option 1 CONUS	$ 27,388.80
Training Option 1 OCONUS	$ 27,388.80
Training Option 2 CONUS	$ 27,388.80
Training Option 2 OCONUS	$ 27,388.80

PURCHASE REQUEST NUMBER: DGEMZ49877

ACRN AA Funded Amount	FFP total	$3,657,680.55

FOB: Destination

ITEM NO	SUPPLIES/SERVICES	MAX QUANTITY	UNIT	UNIT PRICE	MAX AMOUNT
0002		1	Each	$706,048.39	$706,048.39

Information Assurance Support Services
T&M CLIN
DoD-Wide Enterprise Licenses for an automated Information Assurance Vulnerability Management (IAVM) Compliance Tool as in accordance with SOW dated 29 Apr 04 which is an attachment to this order. Period of performance is from 03 Jun 04 thru 02 Jun 05 as in accordance with DigitalNet proposal dated 30 Apr 04 which is incorporated by reference.

MIPR DGEMZ49877

Breakout of support under this T&M clin:

Labor – NTE $550,621.44
Travel – NTE $155,426.95

TOT MAX PRICE NTE CEILING PRICE	$706,048.39
Funded Amount	$0.00

FOB: Destination

ITEM NO	SUPPLIES/SERVICES	MAX QUANTITY	UNIT	UNIT PRICE	MAX AMOUNT
0003		1	Each	$377,052.75	$377,052.75

Option Year 1 Information Assurance Support Services

FFP
DoD-Wide Enterprise Licenses for an automated Information Assurance Vulnerability Management (IAVM) Compliance Tool as in accordance with SOW dated 29 Apr 04 which is an attachment to this order. Period of performance is from 03 Jun 05 thru 02 Jun 06 as in accordance with DigitalNet proposal dated 30 Apr 04 which is incorporated by reference.

Support will include:

Maintenance	$315,147.90
Help Desk Option	$ 61,904.85

	FFP PRICE	$377,052.75

Optional

0003AA	Secure IIS and IRIS Task 6.1	$217,210.00
	Funded Amount	$0.00

FOB: Destination

ITEM NO	SUPPLIES/SERVICES	MAX QUANTITY	UNIT	UNIT PRICE	MAX AMOUNT
0004		1	Each	$388,405.46	$388,405.46

Option Year 2 Information Assurance Support Services

FFP
DoD-Wide Enterprise Licenses for an automated Information Assurance Vulnerability Management (IAVM) Compliance Tool as in accordance with SOW dated 29 Apr 04 which is an attachment to this order. Period of performance is from 03 Jun 06 thru 02 Jun 07 as in accordance with DigitalNet proposal dated 30 Apr 04 which is incorporated by reference.

Support will include:

Maintenance	$326,500.61
Help Desk Option	$ 61,904.85

FFP PRICE	$388,405.46

Optional

0004AA	Secure IIS and IRIS Task 6	$217,210.00
	Funded amount	$0.00

FOB: Destination

ITEM NO	SUPPLIES/SERVICES	MAX QUANTITY	UNIT	UNIT PRICE	MAX AMOUNT
0005		1	Each	$400,240.72	$400,240.72

Option Year 3 Information Assurance Support Services

FFP
DoD-Wide Enterprise Licenses for an automated Information Assurance Vulnerability Management (IAVM) Compliance Tool as in accordance with SOW dated 29 Apr 04 which is an attachment to this order. Period of performance is from 03 Jun 07 thru 02 Jun 08 as in accordance with DigitalNet proposal dated 30 Apr 04 which is incorporated by reference.

Support will include:

Maintenance	$338,335.87
Help Desk Option	$ 61,904.85

FFP PRICE $400,240.72

Optional

0005AA	Secure IIS and IRIS Task 6.1	$217,210.00
	Funded amount	$0.00

FOB: Destination

ITEM NO	SUPPLIES/SERVICES	MAX QUANTITY	UNIT	UNIT PRICE	MAX AMOUNT
0006		1	Each	$411,607.63	$411,607.63

Option Year 4 Information Assurance Support Services

FFP
DoD-Wide Enterprise Licenses for an automated Information Assurance Vulnerability Management (IAVM) Compliance Tool as in accordance with SOW dated 29 Apr 04 which is an attachment to this order. Period of performance is from 03 Jun 08 thru 02 Jun 09 as in accordance with DigitalNet proposal dated 30 Apr 04 which is incorporated by reference.

Support will include:

Maintenance	$349,702.78
Help Desk Option	$ 61,904.85

FFP PRICE	$411,607.63

0006AA	Optional	
	Secure IIS and IRIS Task 6.1	$377,052.75
	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:	Total of order	$4,420,190.72	MIPR DGEMZ49877

CLAUSES INCORPORATED BY FULL TEXT

DITCO Points of Contact

Contracting Officer

Contract Specialist

CONTRACTOR Point of Contact

Contractor Name: DigitalNet
DUNS: 0175301720
CAGE CODE: 0GS16
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 I - Contract Clauses

CLAUSES INCORPORATED BY REFERENCE

52.227-19	Commercial Computer Software- Restricted Rights	JUN 1987

Section J - List of Documents, Exhibits and Other Attachments

SOW DATED 29 APR 04

'I ASSURE' TASK ORDER (TO) STATEMENT OF WORK (SOW) as of 29/APR /2004

Contract Number:	*(completed by the KO at time of TO award)*
Task Order Number:	*(completed by the KO at time of TO award)*
IAssure Tracking Number:	*00232.00*
Follow-on to IAssure 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

DoD-wide Enterprise License for an automated Information Assurance Vulnerability Management (IAVM) Compliance 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 are most often the result of a flaw in the coding of software. As systems and applications become more complex, the number of lines of code multiplies exponentially. Consequently, the potential for flaws also multiplies. By exploiting software vulnerabilities, hackers can spread malicious code that can cause significant and pervasive damage. Vendors, users, researches, and hackers often discover vulnerabilities in existing systems or applications. To rectify the problem, vendors often issue a short-term fix in the form of a patch or recommended change to protocol. Then, vendors incorporate design changes in later versions of the software.

While the threat to 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
- Non-disruptive to Normal Operations
- Accountability and Enforcement
- Training Support for IAVA Implementation
- An Enterprise View of Vulnerabilities

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 IAVM tool that will provide network administrators and security personnel a mechanism for verifying application or non-application of Department of Defense (DoD) Computer Emergency Response Team (CERT) Information Assurance Vulnerability Management Notices as well as vulnerability notices published by the five Service CERT/CIRTs. DoD CERT notices include Information Assurance Vulnerability Alerts (IAVAs), Information Assurance Vulnerability Bulletins (IAVB) and Information Assurance Vulnerability Technical Advisories (IAVTAs) (A/B/TA) DOD CERT and Service CERT/CIRT notices will here after be referred to as “IAVM Notices”. This tool will be applied Enterprise-wide across the DoD, Coast Guard, National Guard, and the Reserves here after referred to as “The ENTERPRISE”. All “ENTERPRISE” owned and leased computers, personal electronic devices, and networks are covered under this agreement, regardless of the persons operating the computer systems. This capability should fully integrate IA Vulnerability identification, verification, and reporting 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. Objectives

4.1 IAVM Objective

Specifically, the IAVM compliance tool is striving to meet the following objectives:

- Provide “The ENTERPRISE” with the ability to assess the IAVM Notices of DoD Information Systems to emerging threats.
- Provide a repository for “The ENTERPRISE” to acknowledge receipt of, provide compliance information to, and view enterprise wide program compliance with the Information Assurance Vulnerability Management Process.
- Provide a tool for “The ENTERPRISE” to notify their organization of specific vulnerabilities using Common Vulnerability Exposure (CVE) and Open Vulnerability Assessment Language (OVAL) names.
- Accept configuration and vulnerability-related checking requirements provided by DoD expressed on OVAL eXtensible Markup Language (XML) when available.
- Provide the ability to quickly notify and receive acknowledgement from subordinates of an emerging threat or vulnerability.
- Monitor status and closure to emerging and known vulnerabilities at the asset level.
- Provide controlled access to vulnerability findings related to computer systems.

- Allow System Administrators (SAs) with the ability to conduct self-assessments of known vulnerabilities on all system assets and track the status through closure.

4.2 IAVM 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)

5.0 Scope

The CVE dictionary of named vulnerabilities is readily available on the public cve.mitre.org web site. 103 vendors have declared that some 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."

Due to the fact that the “ENTERPRISE” IA notice numbers are available only to .mil systems and not the commercial marketplace, the Government will have the option to test the contractor’s submitted products for the IAVM Compliance Tool capability. This test if performed will be conducted in two parts. Part I (pre-award) will test the tool's discovery of vulnerabilities using CVE numbers as well as all other requirements stated within this SOW. One IAVM Compliance tool will be selected as “best of breed” to continue testing in part II (post award). Part II testing will validate that the “ENTERPRISE” IAVM notice numbers have been incorporated into the IAVM Compliance tool by the contractor 20 days after contract award. This will safeguard the “For Official Use Only” (FOUO) nature of the “ENTERPRISE” IAVM notice numbers.

The work is focused in the following areas:

- Provide an automated IAVM tool for both “The ENTERPRISE” that fully integrates IAVM notice identification, verification, and reporting while providing a cost effective training method to employ the technology.

- Provide access to this IAVM tool in the form of an “enterprise-wide” license.

- Provide training and technical support for the automated IAVM tool.

- Comply with the appropriate DoD-approved architectures, programs, standards and guidelines: (such as DII STG, COE, STIG, and DISN).

- Ensure the product is in the process of or has obtained a minimum level of Evaluation Assurance Level (EAL) 2 of National Information Assurance Partnership (NIAP) Certification.

- Conduct Progress Reviews and Project Briefings.

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 – IAVM Tool Solution Installation/Operations
- Task Area 4 – Education, Training and Awareness, Information Assurance (IA) Technical Support, and Contractor Priced Options

6. Specific Tasks

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

6.1.1 Subtask 1 - Integration Management Control Planning

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 provide all software and documentation to the government.

Deliverable: 1. Software and documentation due one (1) working day after the award of the TO.

6.1.2 Subtask 2 - TO Management

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 One (1) working days after the award of the TO.
2. MSR due NLT ten (10) working days after the end of the contractor's monthly accounting period.

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 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/Project Briefings

The contractor shall conduct a formal In Progress Review (IPR) on day 20 of task award and bi-weekly for the first 60 days thereafter on a monthly basis. The contractor's Technical Task Leader (TTL) and appropriate members of the technical team will meet with the appointed Government TM, either in person 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. The contractor shall document these meetings in Quarterly Review Notes and report the occurrence(s) of these and any other meetings in the MSRs.

Deliverable: 1. Bi-Weekly/Monthly Progress Review briefings.
2. Bi-Weekly/Monthly 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.

6.1.8 Subtask 8 – Enterprise License

The contractor shall provide an unlimited enterprise license 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 utilize a source that provides the best value to the Government.

We would also like to obtain favorable 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. 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 ensure that upon submission they have proof of contract seeking NIAP approval or be NIAP approved at EAL 2 or greater.

The contractor shall ensure that each major release of the software is subjected to the NIAP Certification.

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 IAVM tool and all functionality adheres to the applicable DISA STIG to include approved extensions. STIGs are available from http://csrc.nist.gov/pcig/cig.html.

6.2.3 Subtask 3 – IA Vulnerability Schemes and ODBC Compatibility

The contractor shall incorporate all "ENTERPRISE" numbering schemes within their tool keying on the DoD IAVM notice number. These schemes include DoD CERT, NAVCIRT, AFCERT, ACERT, MARCIRT, and CGCIRT Vulnerability. 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.

The contractor shall incorporate both an exportable (comma separated value (CSV)) and ODBC capability within its scanning product. Format for the CSV file will be provided upon contract award.

Deliverable: 1. Contractor will provide DoD IA Vulnerability schemes and ODBC capability within twenty (20) days of award date.

2. Contractor will provide the OVAL XML features in the tool within 12 months of contract award.

6.2.4 Subtask 4 – Hierarchal Architecture

The contractor shall ensure that its IAVM Compliance tool is capable of being deployed on all networks within each "ENTERPRISE" enclave to assess IA vulnerability Compliance. This tool shall have the capability to share the results of its IA vulnerability assessments with many report-generating systems.

The compliance tool will have the ability to run tests within the enclave under both local and external control. The tool must also provide both local and remote reporting with the remote reporting capability designed to incorporate multiple levels of correlation. All out of enclave communications need to be encrypted in accordance with FIPS 140 standard. The ultimate goal is to have the tool input to the Vulnerability Management System (VMS) for vulnerability tracking of assets.

A report-generating system will be deployed at a defined "Headquarters" of a major organizational command element within "The ENTERPRISE" for the purpose of viewing Vulnerability Compliance reports for the entire command.

The tool and report-generating system shall also be accessible via an ODBC data source in order to report the results of their compliance assessments to a reporting database in order to produce Vulnerability Compliance reports across "The ENTERPRISE".

6.3 Task 3 - IAVM Tool Solution Installation/Operation

The contractor shall ensure that the capability fully integrates IA Vulnerability identification, verification, and reporting 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 COE.

6.3.1 Subtask 1 - Automated Vulnerability Identification, Asset Identification and Reporting

The contractor shall ensure that SAs have the capability within the tool that automates the tasks of asset identification, IAVM notice Vulnerability identification, and IA Vulnerability reporting. 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 contractor shall ensure that the tool has the capability to scan 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 address).

New vulnerabilities surface on a regular basis and these tools must keep abreast of these changes. New vulnerability alerts must be continually updated to be able to validate the solutions and links required for remediation of all vulnerabilities. All DoD IAVM Notices are currently stored in a vulnerability database, and new ones are added as they are released. The contractor shall ensure that its tool allows for the storage of all IAVM information in an ODBC-addressable database. DoD IAVM Notices are only available to .mil sites and not the commercial marketplace.

Upon award of contract, the vendor shall provide the DoD CERT IAVA Team with a group email address (i.e., IAVA@vendor.com) in which to send IAVM Notices. The DoD CERT IAVA Team will add this email address to its Precoordination list and send the vendor advance copies of notices prior to Publication.

The contractor shall provide updates to IA Vulnerability notices within 48 hours of release by DoD CERT, 96 hours by agencies identified in CJCSI 6510.01C. The government will test the release and provide updates to “The ENTERPRISE”. If failures are encountered the contractor shall have 24 hours to correct the failure. The contractor provided software shall have a verification method such as an approved digital signatures for validation of authenticity.

The contractor shall ensure that the tool has the capability to generate reports automatically for display on a web page as well as be capable of building selectable reports. The contractor shall ensure that the tool includes a report capability that will be available to users from any machine with a DoD PKI enabled approved web browser. The contractor shall ensure that the tool includes differential reporting capabilities based on a host, scalable group of hosts, or vulnerability with customizable scans for IAVM Notices compliance and service configurable scans. The contractor shall ensure that the tool include a hierarchical reporting capability where security restricts the user to their approved level of authority.

Deliverables**:** IA Vulnerability notices within 48 hours of release by DoD CERT.

6.3.2 Subtask 2 - Field Proven Tools

Vulnerability assessment must determine IAVM notice compliance on a network. The contractor shall ensure that the tool is coupled with a central reporting capability and provides an effective means to identify IA Vulnerability compliance. 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 works in deployable, tactical, and isolated units in remote theaters.

6.3.3 Subtask 3 - Non-Disruptive to Normal Operations

The contractor shall ensure that the tool is able to run on live networks during normal operating hours without affecting the user's mission. This tool must be able to be used during normal operating hours so there is no need to scan at night while users are away and there is a worry about machines being turned off during off-duty hours. The contractor shall ensure that the tool will not be disruptive to the operating environment.

6.3.4 Subtask 4 - Accountability and Enforcement

The contractor shall ensure that the tool allows for IAVM Notices status reports to be entered into one or more “ENTERPRISE” IA Vulnerability repositories.

Examples of information that shall be presented in the status report are as follows:

- IA Vulnerability Alert, Bulletin and Technical Advisory compliance data on network assets within the SA’s purview
- Date scan was performed. Begin and end scan timestamp, scan lapse time (amount of time it took to scan)
- The version of the products used to perform the scan

6.3.5 Subtask 5 - Organizational View of IA Vulnerability Compliance

The contractor shall ensure the following:

The Security Manager in an organization shall be provided with an organizational view of its security posture. Query capabilities, such as Show-me the status of an X IA Vulnerability on X platform, shall be provided within an organizational view by the IAVM compliance tool.

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

6.4.1 Subtask 1 - Training Support for IAVM

Past implementation experience deploying IA tools within “The ENTERPRISE” has proven that without training, a large percentage of those tools remain on the shelf and do not get used, resulting in a poor return on investment. In addition, most IAVM mechanisms are powerful tools that, if not properly employed, have the potential to harm a network with a single click. To provide an IAVM specific training tool, the contractor shall provide a capability for virtual, interactive, on-demand IA training to "The ENTERPRISE” from their duty location/organization computers. Students shall be able to log into this virtual interactive classroom using a number of teaching tools (e.g., streaming video/audio, online classroom chat, web boards, and virtual servers). Students shall be able to log into a virtual classroom from anywhere in the world. Following completion of the on-line training the student will be tested to ensure adequate understanding of the IAVM tool is obtained. It is imperative that students learn to run the IAVM tool and do IA Vulnerability compliance reporting on a virtual network before ever touching their real network. The contractor shall ensure that the tool compliments any formal structured IAVM training presented at any DoD IA training schools. The contractor shall maintain updates to this online training through the life of the contract.

The contractor shall be responsible to update the online training with the release of every major software update and changes determined during a monthly review of the online training. These updates shall be completed within 5 days. Whenever changes occur in the tool the training should be updated, reducing the lag time that now occurs in updating/improving individual technical skills. The Training Server Platform will be in the DISA enclave.

Deliverables**:** Online training package and certification test.

6.4.2 Subtask 2 - Classroom Training Support.

The contractor shall provide instructors who have expert knowledge of and experience with the IAVM tool. The contractor is to provide IAVM classroom training to various "ENTERPRISE" (CONUS/OCONUS) locations. For planning purposes, each course will be delivered 4 times a month at "ENTERPRISE" sites. The classroom training is intended to be given to the core team from Combatant Commands, Services and Agencies-

CONUS –	Four Classes
OCONUS –	Pacific Area of Responsibility (AOR) – Two Classes
	Europe AOR - Two Classes
	Southwest Asia (SWA) AOR – Two Classes

The contractor shall provide a hands-on training environment that will accommodate up to 250 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, and software to support 25 students. Following completion of the classroom training the student will be tested to ensure adequate understanding of the IAVM 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 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: Course Materials (Screen shots, Student handbook, Critique, etc.), Trainer Certification test and After Action Reports submitted for approval by day 20 after award.

6.4.3 Subtask 3 - Technical Support for IAVM Compliance Tool

The capability will be available to the Government that a base level support is provided at a minimum of 8 am to 8 pm EST, Monday through Friday. Technical support to include at a minimum; Level three phone support (this means identify, isolate, and resolve software anomalies). A maximum of 200 calls per month.

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

6.4.4 Subtask 4 - Support for IAVM Compliance Tool During 60 Day Rapid Deployment Plan (See section 9)

The contractor shall provide on-site technical support for 60-Day Rapid Deployment Plan as requested by the Government. This at a minimum will include 80 hours.

Deliverable: 80 hours of technical support.

6.4.5 Subtask 5 – 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.

6.4.5.2 – Contractor Help-Desk Option

The contractor shall provide"one stop" help desk solution. This will be a 24x7x365 help desk. This process must maintain the certification and accreditation process. A minimum support criterion is listed below.

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

6.4.5.3 – Additional Contractor Training Option

The contractor shall provide a cost estimate to satisfy additional classroom training for 100 seats. The training shall be conducted throughout "The ENTERPRISE". Please break down the training options in the following manner:

OPTION 1:

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

OPTION 2:

CONUS –	40 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. Also please provide the Government on price discounts based on the number of seats/personnel to be trained.

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.

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. Since the I-ASSURE contract vehicle is in its 4th year (option year 1 with 3 Option years remaining) rates will have to be negotiated for the last year of this order. 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.

Pre Award

The government will have the option to test the IAVM Compliance Tool solution. If the government elects to test the tool solutions the contractor will be required to provide a fully functional compliance tool to include STIG compliant. The test location will be determined by the government.

Post Award

60-Day Rapid Deployment

- **Day 1** Software, Hardware to support 3 tool suites for 5 test locations, and **and Documentation delivery**
- **Day 1-10 Security test & IATO**
- **Day 5 (NLT) Conduct TIM**
- **Day 10 Begin Phase I**
  - **One Combatant Command**
  - **CVE-based reporting**
  - **Off the shelf Training**

- **Day 20 Phase I IPR**
- **Day 30 Phase II**
  - **One site per Service**
- **Day 60 Full Operational Control (FOC)**

10. Delivery Schedule

SOW Task #	Deliverable Title	Format	Due Date	Copies	Distribution	Frequency and Remarks
6.1.1	Software and documentation Delivery	Electronic	Working days after TO award: 1			
6.1.2	Management Plan	Contractor Format	Working days after TO award: 5			
6.1.2	Bi-Weekly Status Report	Contractor Format	Working days after Bi-Weekly review Notes: 5		Standard Distribution* ***Business Office	
6.1.3	Technical Interchange Meeting	N/A	Calendar days after TO award: 5			
6.1.3	TIM notes	Contractor Format	Working days after TIM: 5			
6.1.4	Bi-Weekly/ Monthly Progress Review Briefings	Contractor Format	Calendar days after TO award: 15/30			15/30 days after contract award for the first two (2) months and monthly thereafter.
6.1.4	Bi-Weekly/ Monthly Progress Review notes	Contractor Format	Working days after the Bi-Weekly/			

			Monthly Progress Review: 5			
6.2.3	ENTERPRISE IA Vulnerability numbering and ODBC integration	DoD CERT IA Vulnerability scheme	Calendar days after TO award: 20			
6.3.1	IA Vulnerability notices	TBD	Within 48 hours of release by DoD CERT.			
6.4.1	Online Training/ Certification Package	Contractor Format	Calendar days after TO award: 20			
6.4.3	On-site Tech Support 80 hours	N/A	At Government Request			
6.4.5	Classroom Course Materials	Contractor Format	Calendar days after TO award: 20			
6.4.5	After Action Report	Contractor Format	Working days after class has been completed: 5			
* Standard Distribution: 1 copy of the transmittal letter with the deliverable to the Primary TM						

* 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

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 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 certified quality management processes (e.g. ISO 9001, Capability Maturity Model, etc.) to evaluate, measure, report, and improve IA Watch Team 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 to accomplish 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 IAVM compliance tools and technologies. Information shall be provided to the government during the month progress review briefings.

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.

14. <u>Section 508 Accessibility Standards</u>. 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

15. 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.

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 `metalanguage' -a language for describing other languages-which 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 metalanguage 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.

IAVM Notice. Any notice published by the DoD CERT or the SERVICE CERT/CIRTs that identify vulnerabilities that poses a significant threat to the ENTERPRISE. This includes: DoD CERT Information Assurance Vulnerability Alerts (IAVAs) Information Assurance Vulnerability Bulletins and Information Assurance Vulnerability Technical Advisories IAVB/TAs) (A/B/TA)s.

IA Vulnerability. DoD CERT Information Assurance Vulnerability Alerts (IAVAs) 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 Vulnerability Management (IAVM) Program. The comprehensive distribution process for notifying Combatant Commanders, Services and Agencies (CC/S/A) about vulnerability alerts and countermeasures information. The IAVM Program requires CC/S/A receipt acknowledgment and provides specific time parameters for implementing appropriate countermeasures depending on the criticality of the vulnerability.

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.

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.

Service CERTs. Army CERT (ACERT) at Ft. Belvoir, VA, Air Force CERT (AFCERT) at Lackland Air Force Base, TX, Navy CERT (NAVCERT) 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.