

AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT

1. CONTRACT ID CODE PAGE OF PAGES

1 11

2. AMENDMENT/MODIFICATION NO. 0001		3. EFFECTIVE DATE 4 SEP 2002	4. REQUISITION/PURCHASE REQ. NO.	5. PROJECT NO. (If applicable)
6. ISSUED BY CONTRACTING OFFICER NAVAL RESEARCH LABORATORY 4555 OVERLOOK AVENUE SW WASHINGTON, DC 20375-5326 ATTN: CODE 3220.CR		CODE N00173	7. ADMINISTERED BY (If other than Item 6) CODE	

8. NAME AND ADDRESS OF CONTRACTOR (No., street, county, State and ZIP Code) TO ALL OFFERORS		(X)	9A. AMENDMENT OF SOLICITATION NO. N00173-02-R-CR11
		X	9B. DATED (SEE ITEM 11) 9 AUG 2002
			10A. MODIFICATION OF CONTRACT/ORDER NO.
			10B. DATED (SEE ITEM 11)
CODE	FACILITY CODE		

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offers is extended, is not extended. Offers must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended, by one of the following methods:
 (a) By completing items 8 and 15, and returning 2 copies of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted; or (c) By separate letter or telegram which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment your desire to change an offer already submitted, such change may be made by telegram or letter, provided each telegram or letter makes reference to the solicitation and this amendment, and is received prior to the opening hour and date specified.

12. ACCOUNTING AND APPROPRIATION DATA (If required)

13. THIS ITEM ONLY APPLIES TO MODIFICATION OF CONTRACTS/ORDERS. IT MODIFIES THE CONTRACT/ORDER NO. AS DESCRIBED IN ITEM 14.

CHECK ONE	A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: (Specify authority) THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NO. IN ITEM 10A.
	B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES (such as changes in paying office, appropriation date, etc.) SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(b).
	C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF:
	D. OTHER (Specify type of modification and authority)

E. IMPORTANT: Contractor is not, is required to sign this document and return _____ copies to the issuing office.

14. DESCRIPTION OF AMENDMENT/MODIFICATION (Organized by UCF section headings, including solicitation/contract subject matter where feasible.)

See Page 2

Questions should be directed to Alan W Crupi, Contract Specialist at (202) 767-3595.

Except as provided herein, all terms and conditions of the document referenced in Item 9A or 10A, as heretofore changed, remains unchanged and in full force and effect.

15A. NAME AND TITLE OF SIGNER (Type or print)		16A. NAME AND TITLE OF CONTRACTING OFFICER (Type or print)	
15B. CONTRACTOR/OFFEROR (Signature of person authorized to sign)	15C. DATE SIGNED	16B. UNITED STATES OF AMERICA (Signature of Contracting Officer)	16C. DATE SIGNED

The purpose of this amendment is to answer questions from potential offerors.

1. Question: What is the expected percentage or amount of overtime ?

Answer:

It would not be expected that the amount of overtime would exceed 10%. It will be driven by the tasking and special efforts associated with the taking. The special efforts will consist of preparation efforts to support program reviews or security assessment that cannot be finished during normal hours of operation.

2. Question: What is the size of the HPCMO enterprise (e.g., number of personnel, workstations, server/mini/mainframe systems, etc.)

Answer:

The HPCMO consists of about 35. Each person generally has one computer. There are two Unix servers to support the operation and a Windows server. The HPCMO consists of support of 12 project centers and 4 major shared resource centers. Connections are maintained to about 80 sites that support approximately 5000 users of the programs supercomputing assets.

3. Question: What components compromise HPCMO's equipment and programs to be reviewed ?

Answer:

The HPCMO security system are those programs managed and directed by the HPCMO for the HPCMP. The HPCMO manages a 24 hour, 7 day a weeks Computer Emergency Response Team (HPC CERT) consisting of approximately 20 full time personnel and augmented by approximately 25 Army Reservists. There are over 35 sensors distributed throughout DREN and centers. The management, procurement, and maintenance of these sensors are the responsibility of the HPCMO. The HPCMO manages and participates in comprehensive security assessments that go to each high performance computing center (~16 centers) and all SDREN sites (~25) on a regular evaluation schedule. In addition, each site connected to the DREN is a viable candidate for an assessment. Currently there are three assessment teams consisting of 3-5 people that conduct the assessments; an HPCMO representative is a member of each team. The HPCMO manages the implementation of wide area network access controls through the support of the AT&T DREN Intersite Service Contract (DISC) and follow-on MCI DREN contract including Access Control Lists (ACLs) and INFOCON situations. The HPCMO is

responsible for managing and developing the access control/authentication policy for high performance computing assets. This includes development of kerberos and PKI implementations. The HPCMO is also responsible for the development/implementation of IAVA compliance, evaluating new tools or techniques, and strategies for protecting the high performance computing assets, the DREN network, the security infrastructure, and/or users systems. The HPCMO security team is also responsible for the accreditation of the DREN, SDREN and the HPCMO DREN and SDREN nodes.

4. Questions: (a) What is the current size and makeup of the HPCMP security Assessment Team? (b) Are there plans to modify or augment the makeup of this group prior, during, or after the award of this contract ?

Answers:

(a) The HPCMP security Assessment Teams consists of 3-5 personnel. Generally, there is a team lead that is responsible for all site visit coordination, collecting all assessment findings, briefing the site on findings and preparing he assessment report. He is also responsible for verifying the findings of others on the team. The HPCMO representative acts to manage the assessment adjust the scope, interpret the HPCMP policies and interface with the HPCMO in cases requiring further adjudication. There are 1 to 3 technical analysts that execute scans and scripts on site systems looking for vulnerabilities. The number depends on the complexity and nature of the site assets.

(b) There are no plans to alter the makeup of the assessment teams. The person involved in this effort will act as an HPCMO representative to interpret HPCMP policy and interface with the Security team at the HPCMO.

5. Question: In Section 3.2 of the SOW it is stated "The contractor shall provide support to the HPCMP Security Assessment Team" - will this support be managerial in scope, or technical, or both ?

Answer:

The contractor will act as an HPCMO representative on the team. The scope will be both technical and managerial. The technical portion will be as communications systems analysts to assess the proper utilization of the DREN by the site and the proper controls of the networking equipment. Ultimately the HPCMO representative is responsible for the validity of the assessment and providing the report to the HPCMO. This person also acts to grant interim authorities to connect the site to DREN at the conclusion of the assessment. Conversely, this person also authorizes the disconnection of sites if the findings are too severe.

6. Questions: (a) Has the CSA test plan been developed ? (b) If so, can that be made available to assist in determining level of effort in the bidding process ? (c) What is the approximate number of sites to be visited ?

Answers:

(a) Yes the test plan is developed.

(b) No, It is for official use only and can't be released because of proprietary issues as well as sensitivity. The level of effort is dictated by the nature of the site. A Major Shared Resource center will be a 2-3 week effort. A shared resource center will be a 1-2 week effort. SDREN sites will be roughly a 1 week effort.

(c) There are approximately 30 comprehensive Security Assessments per year. There would not be anticipated to be more than 10 sites that the contractor would be required to participate.

7. Question: What is the current HPCMP storage and retrieval process ?

Answer:

The current HPCMO process involves having all of the information gathered during the assessment being included in the formal report.

8. Question: What extent will the contractor's involvement be in the C&A process ?

Answer:

There is accreditation documentation for the DREN, SDREN, and HPCMO DREN and SDREN node. There is also accreditation documentation that is being prepared for the DREN2 Worldcom contract. To the large extent someone else will prepare the documents but there will be review and suggestions for revisions required.

9. Question: What CERT capabilities are currently in place and/or utilized by HPC users ?

Answer:

The CERT is currently in place and functional. The following are the activities defined for the CERT: Provide "24 x 7" intrusion detection and monitoring services. Near-real time – Near-real time monitoring is defined as the detection and notification within 30 minutes of the occurrence of an event. The events identified for near-real time detection and notification pose an imminent threat to a system or site. Notification is promulgated to the affected site and the HPCMO.

Retrospective – Retrospective analysis is the detection and notification of the occurrence of an event that cannot easily be characterized or detected by near-real time software. Retrospective analysis is also analysis that is performed as a further investigation of events that were identified by a real time notification, or as a detailed analysis of the entire volume of data collected from the sensor.

Retrospective analysis is used to identify events that emerge from a detailed analysis of captured data. All initial incident reporting must be done within 24 hours of the incident occurring. Data correlation and fusion – It is required that data obtained from the sensors be maintained in an active state for one year and that sensor data be archived for at least two years. Data correlation and fusion techniques will be used to identify trends in the stored data. Identified trends will be reported to the HPCMP community and DOD CERT community as they emerge or in periodic reports.

Data security of monitoring devices – The monitoring devices provide a unique view of data transiting a site connection. The security of the monitoring devices is essential. Techniques will be employed to minimize the profile of the device, restrict the access to the device, and record interactions with the device. The security of the monitoring devices shall be reviewed before shipment and reassessed periodically, while in the field. The sensor supplier will follow approved DISA security guidelines in preparing the sensor and perform a Security Readiness Review (SRR) minimally on each sensor platform configuration. The HPC CERT will review the results of the SRR and recommend additional enhancements as necessary. Once fielded, the HPC CERT will review the security of the monitoring device periodically and update the Operating System appropriately with known patches. Access to the devices will conform to established HPCMP access procedures. The system logs employed to monitor the interactions with the monitoring devices will be reviewed daily.

Data security of the archive server at HPC CERT - The archive servers provide a unique aggregation of data transiting the DREN. The security of the archive servers is essential. Techniques will be employed to minimize the profile of the servers, restrict the access to the servers, and record interactions with the servers. The security of the archive servers should be reviewed before deployment and reassessed periodically while in the field. The archive servers will be prepared for deployment with the approved DISA security guidelines, and an SRR will be performed prior to deployment. The HPC CERT will review the results of the SRR and provide additional enhancements as necessary. Once fielded, the HPC CERT will review the security of the archive servers periodically and upon any configuration change. Access to the devices will conform to established HPCMP access procedures. The system logs employed to monitor the interactions with the archive servers will be reviewed daily.

Review router logs/reports, analyze the data, and use to improve monitoring – The routers deployed in the DREN may have the ability to provide reports or logs of transactions handled by the router. This router data provides information that will supplement the data collected from monitoring devices and can be useful

when correlated with the monitoring device data to determine the effectiveness of access control lists and attack signatures deployed on the monitoring devices. When available, the HPC CERT will integrate the data collected from the routers into the analysis process.

Coordinate with site POCs to encourage reporting of any suspicious events – Reports from the site POCs provide an additional source of information. The HPC CERT will encourage the site POCs to provide event information to the HPC CERT especially when HPC resources are involved including attacks that use the DREN for access.

Provide intrusion detection sensor performance statistics identify and isolate conditions where sensors fail to collect information – The performance of the sensors must be monitored to determine the health of the devices. Sensor performance also must be monitored to determine anomalies that may occur in the data traffic patterns. The HPC CERT shall correlate the data from the sensor performance collection tools to identify trends. Sensor performance statistics and trends shall be reported weekly.

Participate in the repair or replacement of intrusion detection devices – The HPC CERT will perform all necessary tasks to maintain the sensors in an operational state. The HPC CERT will track the duration of sensor failures, document the corrective actions taken to restore the sensor, and record the duration of assistance provided by external sources (such as AT&T or the sensor supplier). Intrusion detection sensor configuration and coordination activities. Ensure appropriate response to events – The HPC CERT will employ the DOD methods of categorization. All category 1, 2, and 5 events require a response from the affected site's personnel to indicate the actions taken and the resolution of the event. Similarly category 7 events will be tracked when it appears the event is unique (close coordination with DOD CERT may be required to identify unique events of interest in this category.) The HPC CERT will track actions associated with the event response until the conclusion of activity on the event. The HPC CERT will provide a summary of all closed events and will provide periodic status (not to exceed one month) on all open events.

Apply HPCMP policies (e.g., no SU to root in the clear) – As unique policies are developed, the HPC CERT will be asked to implement them and/or monitor compliance. One such example is the clear text passwords sent through the network. These actions will be identified to the HPCMO and tracked until the affected site provides an appropriate response.

Obtain, prepare intrusion detection device filter lists and templates – The sensors as currently deployed operate by matching an attack signature with the collected data. The signature filters for the Joint Intrusion Detection Systems (JIDS) are updated on a regular basis by the DOD CERT. The HPC CERT must coordinate with the DOD CERT to obtain the updates. The HPC CERT may develop additional signature filters in cooperation with the HPCMO/sites and independently. As necessary signatures unique to the HPC CERT may be shared with the DOD CERT as applicable. Any other signature filter used in the

performance of the HPC CERT functions will be updated as necessary to maintain currency with the threat environment.

Provide threat analysis when adding, modifying, or removing filtering signatures – When the filters are altered the rationale behind the decision and the implementation time will be recorded. The analysis of the threat will be provided to the HPCMO for review.

Coordinate with sites on specific modifications to filtering lists – Sites may request certain modifications to the filter lists associated with their site. The HPC CERT will work with the site to implement site-specific changes. An analysis of the changes will be provided.

Coordinate with the DOD CERT as a Tier II operation – HPC CERT must fulfill the requirement associated with certifying its operation as a Tier II CERT organization. The HPC CERT will review the requirements of applicable DOD policy (CJCSI 6510.01()) and implement the policy. As guidance, the HPC CERT will be familiar with the operational requirements of the DISA Regional CERTs.

Ensure the integrity and confidentiality when coordinating with other organizations – When communicating with other organizations the HPC CERT will ensure that they have a positive identification of the other party before discussing any sensitive information. When sensitive information is transmitted the HPC CERT will use accepted encryption methods.

Assist recovery/restoration of operations following an incident – Following an incident, the HPC CERT will provide the site with remediation assistance.

Assist law enforcement in the event of a compromise – Once an incident is referred to law enforcement agencies, the HPC CERT will provide information as necessary during the conduct of the investigation.

Router/ACL/Filter management. Prepare Access Control Lists (ACL) for HPCMP sites – The task is to coordinate with the various advisory panels and DOD activities to review and recommend changes to the ACLs and participate as necessary in the preparation, management and implementation of ACLs at designated Service Delivery Points (SDPs). The HPCMP employs ACLs at Network Access Points (NAPs). In the future the use of ACLs may be expanded to all sites. Currently the network service provider implements the ACLs for the HPCMP. For NAPs – may require extensive coordination. For sites may require extensive coordination and several different lists based on the type of site. May include blocking individual Internet protocols and/or addresses at specific sites.

Provide a single Point of Contact (POC) – The single POC is responsible for the operational aspects of the HPC CERT. The POC is the HPCMP primary interface at the HPC CERT. The POC is also the primary interface to the HPC CERT's interactions with other organizations related to CERT functions. The POC is expected to have the authority to effect changes and implement corrective actions to ensure the stable operation of the HPC CERT and to ensure that its capabilities evolve to address ever-changing threats. The following is a representative but not exhaustive list of the responsibilities and activities of the POC. Is responsible for all aspects of operation and actions. Evaluates and tracks resolution of all open tickets. Provides periodic reports on activities and

plans for improvement if appropriate. Coordinates/meets with users on a regular basis. Serves as primary interface to DOD CERT. Leads the interface on site issues. Is responsible for developing operating procedures. Is responsible for providing verifiable contact information and identifying HPC CERT personnel. Is responsible for security clearance of personnel (Secret minimum). Is responsible for ensuring secure communications. Is responsible for ensuring accuracy and timeliness of reports. Is responsible for accreditation of the HPC CERT facilities, hardware, and the fielded intrusion detection systems.

Provide alerts and warnings – The HPC CERT will employ a reporting structure designed to alert managers and administrators at all levels concerning Information Assurance (IA). Timely collation, correlation, information analysis, and warning dissemination require a robust reporting structure. The HPC CERT will integrate the various IA information sources with HPCMP specific information to present an IA resource to the HPCMP community and provide situational awareness to sites on the DREN. The HPC CERT should refer to the DISA Regional CERT Concept of Operations for guidance. Keep aware of all CERT community alerts and warnings. Disseminate alerts of interest to the community. Ensure that alerts and warnings are understandable and minimally redundant. Assist in the fielding of intrusion detection sensors – The sensors are currently procured and prepared for deployment through an HPCMO support contract. The HPC CERT will support the deployment by providing the appropriate configuration to the sensor supplier. The HPC CERT is responsible for maintaining the configuration of the sensors and providing the configuration to the HPCMP. Changes to the configuration shall be coordinated through the HPCMP. The HPC CERT will provide approved changes to the sensor supplier to ensure a common configuration of all sensors. The HPC CERT will review the configuration of sensors at shipment to ensure the common configuration and to verify the operability of sensors prior to shipment. Once fielded the HPC CERT will provide support necessary to maintain the health of the sensor. The HPC CERT will monitor the performance, stability, and viability of the sensor in the field and initiate actions to restore sensor health when necessary. Coordinate with HPCMP sensor supplier to maintain a hot spare. Troubleshoot deployment. Provide on-site assistance at location if necessary. Automate software installation processes.

Investigate/develop infrastructure protection systems (hardware and software) to provide improved security to the rapidly changing HPCMP infrastructure – The HPC CERT will evaluate its performance in the face of a changing threat and evolve to address emerging threats. Training – The HPC CERT will ensure that the personnel employed by the HPC CERT maintain and expand their knowledge and abilities through training. The HPC CERT will define training goals for each class of employee and promote their development. The HPC CERT will also have a training mission for the HPC community. At major HPCMP events, the HPC CERT will offer relevant training to the HPC community. Product evaluations – The HPC CERT will stay abreast of product developments in the IA

field. The HPC CERT will evaluate promising technologies to determine their applicability to the HPC CERT mission. The evaluation of products will have a formal structure to ensure proper evaluation and require HPCMO approval before deployment. Software or scripts to automate processes and procedures or reduce manpower – HPC CERT will pursue to processes to extend or enhance capabilities without increasing manpower. Automation will be a key component. The HPC CERT will maintain or enhance the technical expertise of personnel to automate processes and procedures though software techniques. The automation of processes and procedures should evolve with the requirements. Auditing and consulting services – The HPC CERT will provide technical support as a resource of technical expertise to the HPCMO and the HPC community.

10. Questions: (a) There seems to be a CERT in place. Is this the case ? (b) If not, what CERT capabilities are in place ? (c) If so, what is the size and breath of the area of coverage for this CERT ? (d) Which networks, resources and locations would be included ?

Answers:

- (a) The CERT exists and is operational.
- (b) CERT is fully operational and manned.
- (c) It monitors up to 35 sensors on a 24 by 7 basis. The sensors are primarily at Network access points, shared resource centers and peering locations.
- (d) The effort is primarily a support role in the management of the CERT and the evaluation of new tools to implement at the CERT or the network security architecture.

11. Question: What is the intent of coverage and/or integration for the on-site emergent integration for INFOSEC and network related items ?

Answer:

This means that the contractor is required to stay abreast of new developments in INFOSEC and network security techniques and architecture and be able to provide assistance in the integration of these with the current architecture as implemented by the HPCMP and DREN.

12. Questions: (a) What is the current status of HPC's Network Intrusion Detection System (NIDS) ? (b) Is there currently a system operational, or will one need to be researched, selected, configured, tuned and administered from scratch ?

Answers:

(a) There are currently ~35 NIDS deployed in configurations for OC-12, OC-3 ATM and GigE, FastE, FDDI and Ethernet.

(b) The intent is not to go from scratch but rather a matter of making recommendations for enhancements to the configuration.

13. Question: What are the hardware counts of devices needing monitoring and maintenance (broken down by ACL devices and in-line encryptors) ?

Answer:

There are up to 16 possible devices that will have ACLs. There is the potential for ~80 line encryptors. This effort is planned but not currently implemented. The intent is to monitor the status of these devices from a central location. It is not anticipated that this will be an extensive effort as these configurations should not frequently change. It is primarily from a configuration management and maintenance perspective.

14. Questions: (a) Do the Standard Operating Procedures for the CERT currently exist or do they need to be developed ? (b) If they exist, can a copy be provided to help determine the level of effort needed to fulfill this requirement ?

Answers:

(a) The Operating procedures of the CERT currently exist.

(b) These operational procedures are sensitive information and can not be released. The intent is to integrate the services of the contractor into an ongoing effort with and in support of the HPC CERT. The level of effort is not extensive but it is required that it be integrated with the current operation.

15. Questions: (a) In reference to the SOW Section 3.4 - does this refer solely to the support Network Intrusion Detection System implementation mentioned earlier in section 3.4, or are other Intrusion detection System components currently implemented ? (b) If so, what other IDS components have been implemented, that may need new application support ?

Answers:

(a) This refers to support in the evaluation of a variety of tools including intrusion detection, correlation, integrated management tools, security compliance tools, etc.

(b) The intent is to look at new tools that can benefit the security architecture of the network or systems at centers.

16. Question: Does HPCMO consider an MS Access type database acceptable for the storage and reporting needs required in Section 3.5 of the SOW ?

Answer:

The contractor should be able to do development and support of filemaker databases, currently implemented and have the ability to extend them to meet new requirements. Similarly there are Oracle databases that require similar effort.

17. Question: What is the type, size, complexity of the AEGIS database ?

Answer:

This database consists of an Oracle database with approximately 5000 records. The complexity is fairly simple.

18. Questions: (a) What computer languages are current or future programs written ? (b) Will this support mostly be limited to scripting languages (such as PERL or Shell), or does this include more complex compiled languages, such as C, C++, etc. ? (c) What type or software will require development and/or modifications ?

Answers:

- (a) The languages are C, PERL scripts, filemaker scripts.
- (b) It requires both, but the majority is anticipated to be scripting languages.
- (c) The software that will be modified will be the database interactions to include exchanges between Oracle and Filemaker and the scripts and actions involved.