AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT

1. CONTRACT ID CODE	PAGE OF PAGES	
S	1	32

2. AMENDMENT/MODIFICATION NO.	3. EFFECTIVE DATE	4. REQUISITION/PURCHASE REQ. NO.	5. PROJECT NO.(If applicable)
0002	19-Jul-2016	N6227116RC3A004	

6. ISSUED BY CODE N00244

NAVSUP FLC SAN DIEGO
REGIONAL CONTRACTS (CODE 200)
3985 CUMMINGS ROAD
BUILDING 116 - 3RD FLOOR
SAN DIEGO CA 92136-4200

7. ADMINISTERED BY (If other than item 6) CODE

See Item 6

8. NAME AND ADDRESS OF CONTRACTOR (No., Street, County, State and Zip Code)

CODE FACILITY CODE

X	9A. AMENDMENT OF SOLICITATION NO. N00244-16-R-0009
X	9B. DATED (SEE ITEM 11) 12-Jul-2016
	10A. MOD. OF CONTRACT/ORDER NO.
	10B. DATED (SEE ITEM 13)

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

[X] The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offer [ ] is extended, [X] is not extended.

Offer 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 _____ 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 you 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 APPLIES ONLY TO MODIFICATIONS OF CONTRACTS/ORDERS. IT MODIFIES THE CONTRACT/ORDER NO. AS DESCRIBED IN ITEM 14.

[ ] 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.)

The purpose of this amendment is to add security language into the Performance Work Statement as well as modify 5.0 of Section L. All other terms and conditions of this solcitation shall remain the same.

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) TEL: EMAIL:	
15B. CONTRACTOR/OFFEROR (Signature of person authorized to sign)	15C. DATE SIGNED	16B. UNITED STATES OF AMERICA BY (Signature of Contracting Officer)	16C. DATE SIGNED 19-Jul-2016

SECTION SF 30 BLOCK 14 CONTINUATION PAGE

SUMMARY OF CHANGES

SECTION C - DESCRIPTIONS AND SPECIFICATIONS

The following have been modified:
PERFORMANCE WORK STATEMENT

INFORMATION TECHNOLOGY AND COMMUNICATIONS SUPPORT SERVICES INDEFINITE DELIVERY/INDEFIITE QUANTITY MULTIPLE AWARD CONTRACT

BACKGROUND

The three peer institutions of the Naval Higher Education Information Technology Consortium (NHEITC); the Naval Postgraduate School (NPS), the Naval War College (NWC), and the United States Naval Academy (USNA) have had a 12 year collaboration to enhance the consortium's employment of Information Technology (IT) towards meeting the mission needs of the three member institutions.

The NHEITC is partnering in a strategic IT sourcing solution that will result in a shared 5-year Indefinite Delivery/Indefinite Quantity (IDIQ) Multiple Award Contract (MAC). This approach, as a leading strategic solution for the NHEITC, will provide for a common pool of resources from which to draw for similar services at each institution. This common pool of resources approach will allow the NHEITC schools to best secure their respective .edu networks with complementary overarching security solutions, alternate the institutional leads for the variety of projects both near and long term, create economies of scale, eliminate redundant services, and demonstrate a project driven environment with responsible budget management. In time, as candidate IT services between the NHEITC schools are identified and further migrated to the Cloud, the three member institutions may be able to further pool contract support and create more economies of scale through a flexible control of efforts and resources.

The NHEITC institutions require technical support in 14 critical categories: applications, computer network defense, learning management systems, multimedia educational technologies, virtualization, network and infrastructure maintenance, network engineering, enterprise architecture, service center services, client hardware and lab services, enterprise information, system architecture, system administration, and visualization services.

The NPS located in Monterey, California supports the Department of Navy (DoN), other military branches, and foreign military services with postgraduate education for military and civilian personnel. NPS also provides significant research capabilities to the Department of Defense (DoD). The Information Technology And Communications Services (ITACS) department at NPS is the centralized information technology service provider for the University. ITACS' mission is to provide technology and communications support for the NPS core mission of teaching, research, and service to the DoN and DoD, and to provide voice, video, and data infrastructure as mission-crucial enablers of innovation and experimentation within the educational enterprise.

The Naval War College (NWC) located in Newport, Rhode Island, provides Professional Military Education and Joint Professional Military Education, and helps the Chief of Naval Operations (CNO) define the future Navy, its missions and roles, support combat readiness, and strengthen maritime security cooperation. The Information Resource Department (IRD) is the NWC's centralized provider of information technology services. The mission of the IRD is to provide day-to-day support of the NWC in IT, Video and telecommunications support.

The United States Naval Academy (USNA) located in Annapolis, Maryland is the DoN's undergraduate college for preparing young men and women to become professional officers in the Navy and Marine Corps. The Information Technology Services Division (ITSD) is the centralized information technology service provider for the institution.

ITSD's mission is to develop, manage and integrate technology and communications support for the USNA core mission of moral, mental and physical development of approximately 4,500 midshipmen and 2,500 faculty and staff.

1. IDIQ PWS OVERVIEW

1.1 PLACE OF PERFORMANCE

The services required by this IDIQ MAC shall be performed at NPS, Monterey, CA, at NWC, Newport, RI and at USNA, Annapolis, MD. NPS has satellite offices in Camp Roberts, CA, San Diego, CA, Norfolk, VA, and the National Capital Region (VA, DC, MD) which may require services from this contract.

1.2 INTRODUCTION

The scope of this IDIQ MAC is to provide NPS, NWC, and USNA with support in a variety of disciplines and sub-disciplines within IT. The support services contract is required as the NPS, NWC, and USNA operate their IT environments on government and commercially delivered networks and maintain a minimum of government civilian staff as IT specialists. In order to continue its mission support the NPS ITACS, NWC IRD, and USNA ITSD must obtain contracting services for its IT specialist labor requirements. Contractor services are essential for the successful execution of their mission in support of their respective institutions.

Undergraduate, graduate, and professional education depends on the intellectual enrichment of scholarship and research in order to maintain currency and academic rigor. Research university faculty members teach from existing bodies of knowledge and create new knowledge through inquiry and invention. This means that access to leading edge technology tools is an integral part of the research and education process. It also means that technical support for these tools must be responsive and expert.

Collaborative work, a hallmark of academic research must be supported. Voice, video, and data tools must be available to facilitate partnership across disciplinary, organizational, and geographic boundaries. NPS covers not only a broad international, joint-service resident base, but also a growing group of distance learning (DL) students located throughout fleet concentration areas and throughout the globe. The NWC brings together senior and intermediate level naval officers from other countries to develop leaders for high command in their navies; promote an open exchange of professional views; encourage friendship and cooperation; and study operational planning methods. Meanwhile USNA similarly hosts students of diverse backgrounds and supports an increasing number of students studying internationally.

1.3 Naval Postgraduate School

The NPS curriculum provides a continuum of learning opportunities, including Graduate Degree Programs, Continuous Learning Opportunities, Refresher and Transition Education. These programs are under the auspices of the four graduate schools and the Research Department.

Graduate School of Business & Public Policy
The Graduate School of Business & Public Policy (GSBPP) is responsible for academic programs designed to educate officers and DoD civilian employees in a variety of functional management specialties.

Graduate School of Engineering & Applied Science
The Graduate School of Engineering and Applied Sciences (GSEAS) supports the Navy and the Department of Defense by educating future leaders to lead, innovate and manage in a changing, highly technological world, and by conducting research recognized internationally for its relevance to national defense and academic quality.

Graduate School of Operational & Information Sciences
The Graduate School of Operational & Information Sciences (GSOIS) includes Graduate Resident Programs consisting of 16 technical Curricula and awards Master of Science Degrees and Ph.D. Degrees across four Academic Departments.

School of International Graduate Studies
The School of International Graduate Studies (SIGS) provides high-quality graduate education and conducts research programs focused on international relations and regional security to meet the needs of the nation and our international partners, and to build partnership capacity.

Research Department
One of the major goals of the NPS Research Program is provide cost-effective research and unique laboratory facilities that permit students and faculty to support Navy/DoD needs. NPS provides independent assessments of proposed solutions to military issues, pre-deployment evaluation of new technologies, and combined student-faculty expertise for current research and development programs. Research is conducted in every academic department within the graduate schools and in the research and education institutes.

Each of the university's academic schools as well as NPS' robust research program is led by a Dean providing strategic direction for each organization to achieve the highest levels in academic excellence and relevant research. Throughout the leadership structure at NPS are visionaries capable of marrying high-level, forward-thinking academia with real-world DoD relevance, guiding the university to excel in its unique niche.

In addition to the academic departments NPS is sustained by several administrative groups that provide critical support across varied functional support areas dedicated to high-level, responsible and efficient service to the Naval Postgraduate School and the Navy. NPS' staff directorates oversee the efficient delivery of empowering services to the institution, enabling the NPS community to fulfill its mission of unique academic excellence and relevant research.

1.4 Naval War College
The curriculum at the NWC is based upon three core courses of study: Strategy and Policy, National Security Decision Making, and Joint Military Operations.

Strategy and Policy
The Strategy and Policy course is designed to teach students to think strategically about the theory of warfare from the early battles at sea between Athens and Sparta to the wars of the present day. The focus is on the relationship between a nation's political goals and the way in which its military means are most appropriately used to achieve those ends.

National Security Decision Making
The National Security Decision Making courses are uniquely designed to assist the military and civilian executive dealing with the economic, political, and military factors of decision making in the national security arena. Case studies exploring major contemporary warfare, geopolitical crises, and contingency force-planning issues challenge students to develop the skills to assess the many, often competing, demands involved in the size, shape and budget of future military forces.

Joint Military Operations
The Joint Military Operations course focuses on the translation of contemporary national and regional military strategies into naval, joint, and multinational operations, with particular emphasis on operational art and employment of the sea services. Historical and contemporary case studies and planning exercises permit students to hone their skills in making sound operational decisions, to prepare them for critical command and staff positions.

1.5 United States Naval Academy
The curriculum at the USNA prepares young men and women to become professional officers of competence, character, and compassion in the Navy and Marine Corps. USNA students are midshipmen on active duty in the U.S. Navy. They attend the Academy for four years, graduating with Bachelor of Science degrees and then commissioning as Ensigns in the Navy or Second Lieutenants in the Marine Corps. The curriculum has three basic elements:

Technical
Core requirements in engineering, natural sciences, the humanities and social sciences to assure that graduates are able to think critically, solve increasingly technical problems in a dynamic, global environment, and express conclusions clearly.

Academic
Core academic courses and practical training to teach the leadership and professional skills required of Navy and Marine Corps officers.

Major
An academic major that permits a midshipman to explore a discipline in some depth and prepare for graduate level work.

The Naval Academy policy is to promote and maintain an environment in which research and scholarly activities contribute to the professional growth of faculty and the educational growth of midshipmen.

2. IT ENVIRONMENT

2.1 NPS ITACS

ITACS is comprised of several departments working in collaboration to implement its mission. These departments are: Cybersecurity, Cyberinfrastructure, Enterprise Information Systems, Technology Assistance Center, High Performance Computing, Classified Computing, Educational Technologies, and Resource Management.

ITACS strives to keep all technology current and at the forefront of technological evolution. Systems, applications, equipment, and tools, will change overtime, in some instances gradually as from one version to the next version, or drastically such as moving from one product to a different product. NPS' IT environment is dynamic and is constantly reviewed for relevance, currency, and efficiency.

Cybersecurity
Cybersecurity (CS) is responsible for ensuring the secure operation of the networks and data which includes computer network defense and monitoring, antivirus and vulnerability, operating system and application patch management, and Authorization and Accreditation (A&A) of networks and applications. Staff provide the tools and technologies to find, protect, and react to the unauthorized disclosure of sensitive and privacy data, liaises with third parties through the DoD and DoN, the greater academic community and state and local government organizations to maintain currency with the latest CS and privacy policies, guidelines, threats and vulnerabilities; to deliver relevant and timely training to the campus user population; and to collaborate with faculty and students on CS relevant research topics.

Development Operations
Development Operations (DevOps) has established wide area network connections to the Defense Research and Engineering Network (DREN) and the California Research and Education Network (CalREN). These connections are isolated from each other, adequate to the current and near term data transport requirements, and capable of upgrade to higher speeds at reasonable cost when increased requirements dictate. The primary network, the ERN or .edu is a 10 Gigabit Ethernet (GigE) core backbone in two L2/L3 switches with redundant connections to the Data Center and Distribution Layers. The Data Center Layer consists of seven switches that connect to the various server farms at 10gigE over single mode fiber. The Distribution Layer consists of nine switches that connect to the Core at 10 GigE and to the Edge Layer at 10GigE and 1GigE. The Edge Layer consists of 310 switches and 200 wireless access points providing over 10,000 end user connections. Existing wireless access point inventory does not provide 100% coverage and existing edge layer Ethernet switch count does not activate all current and future end-user ports.

Edge switches are configured as Layer 2 devices. Voice traffic and video traffic is segregated onto separate VLANs. Core and distribution switches are chassis based; edge switches are fixed configuration. Avaya telephone switching equipment supports voice traffic, VOIP telephones are fully supported on an as needed

basis with POE power. Manufacturer developed software is used to manage network electronics. What's Up Gold, Nagios XI, and InMon are used to monitor network performance and health. SNORT, SEP, SafeConnect, SQUID Proxy, 802.1x Wired Port Security are in place to support network security.

The secondary network, DREN is small in scope and consists of one outside router, one firewall, one L2/L3 core switch and, one Data Center switch and connections from ISP to Edge are 1GigE. There is no Distribution Layer and there are only three Edge Layer switches. Most connections are from the mainframe and research projects.

ITACS provides integrated, comprehensive technology solutions that enable NPS to streamline and improve its business processes and practices, including the technical implementation of the NPS public and intranet websites, maintenance and administration of over 50 locally developed commercial web applications, administration of 310 relational database on 30+ instance of database servers; Microsoft Structure Query Language (SQL) server, Oracle, and MySQL, implementation and maintenance of a web-based issue tracking and project management systems; Atlassian's Confluence and Jira, and collaboration tools such as SharePoint and enterprise wiki.

Technology Assistance Center
The Technology Assistance Center (TAC) or helpdesk, provides tier 0, tier 1, and tier 2 customer service to resident, DL, and off campus students, faculty, and staff. The staff responds to walk-in , email, and telephone requests and provides a robust self-help service via the TAC wiki. The TAC is transitioning from eHelpDesk to JIRA Service Desk.

High Performance Computing
High Performance Computing (HPC) manages Linux systems used for teaching and research, provides visualization services that can use the Sony 4K projector to render enormous datasets, and oversees the HPC service. The HPC supercomputer "Hamming" has more than 1,484 computational cores and 6,304 graphical processing unit (GPU) cores.

Classified Computing
Classified Computing (CC) provides staff and infrastructure to support the operations of the university's five classified networks. Leveraging the expertise found in ITACS' other functional areas, CC supports classrooms, computer labs, secure Video Tele-Conferencing (VTC), DL, conferences, and seminars in the Sensitive Compartmented Information Facility (SCIF), Systems Technology Battle Lab (STBL), the Dudley Knox Library, Watkins Hall, and in various campus auditorium and lecture halls.

Educational Technologies
Education Technologies (ET) is responsible for all of the technology, learning spaces, and audio-visual (AV) systems used in teaching both resident and DL students, including oversight of 12 computer labs, 18 VTC VIEO Tele-Education (VTE) systems, 96 smart classrooms, five conference facilities, and 250 software packages. ET maintains the Sakai Collaborative Learning Environment (CLE), web-based collaboration and streaming and on-demand video systems, on-campus podcasting, and the robust VTE infrastructure

Resource Management
Resource Management (RM) provides oversight of human resources: recruitment, retention, professional development and training; budget development and execution; procurements; contracts; office and space management.

2.2 NWC IRD
IRD is made up of six functional divisions: Customer Support Services, Systems Administration, Networks, Application Development, Information Security and IT Business Operations. It provides support in several key areas; web/database/portal development, Tier I/II service desk, instructional systems development for distance education, network technician, telecom technician, information security, systems administration, information

security specialist, desktop management, network video broadcasting, audio/visual systems, and telecommunications functions.

NWC IT Infrastructure

The NWC IT infrastructure includes approximately 93 physical and virtual servers running Windows, OSX, and Linux on four separate backbones (commercial ISP, EDU, DMZ, and SIPRNET) comprising classified and unclassified networks. There are approximately 1400 clients on these networks combined. There is also external connectivity to the SIPRNET and Internet through T1 and 10Gig circuits respectively. The NWC currently uses Microsoft Windows 2008R2 / Windows 2008 / Windows 7 as the network and desktop operating system. Google Apps for Government for the .EDU E-mail system and the use of Microsoft Exchange 2010 is used as the SIPR email system. The application suite currently used is Microsoft Office 2010. The databases used are a combination of Microsoft Access 2003 and Microsoft SQL Server 2008R2. The software versions change to keep pace with technology. All service incidents, problems, resolutions, and change requests are tracked in an incident management system (IT Direct). All systems are deployed configured to the Navy Security Content Automation Protocol (SCAP) standards and Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs) when required.

The NWC has one web server on SIPRNET running Windows 2008 / IIS 7.0, one web server on NIPRNET running Windows 2008 / IIS 7.0, one web server on a DMZ running Windows 2008 / IIS 7.0, and one development web server running Windows 2008 / IIS 7.0. The College also has one SharePoint 2010 portal on the DMZ using claims based authentication tied to our CAC enabled ADFS server and one SharePoint 2007 portal on the SIPRNET. MS SQL Server databases and servers are found through our DMZ, NIPRNET, and SIPRNET networks. Visual Studio 2010 and SharePoint Designer 2010 are the editors for these web sites. There is a mix of Microsoft .NET 2.0 - 4.0 applications and some legacy technologies on our NIPRNET and DMZ web servers. Applications on NIPRNET and DMZ servers utilize ASP.NET, C#, XML and JavaScript technology and connect to MS Access 2010 databases as well as SQL Server 2008 databases. A Google Apps Domain is also used to provide email, intranet websites and document collaboration to users using claims based authentication tied to our CAC enabled ADFS server.

Network Services Branch

The Network Services Branch manages the Firewalls and Cisco network environments on both EDU and SIPRNET networks which are made up of Cisco switches, routers, and access points providing both wired and wireless connectivity to fifteen buildings within the College's campus. The network infrastructure consists of (single/multi-mode) fiber, and CAT6/5e cabling. The telecommunications consist of 1500 analog and digital telephones tied into the Naval Station Newport's Base Communications Office's Central Office switch. NWC is migrating to a Cisco VoIP solution for FY14/15 and will continue with VoIP implementations as our primary voice solution. Multiple Cisco applications are hosted in a virtualized environment that is utilized for the management of the Cisco network environments.

Customer Support Services Desk

Customer Support Services Desk is responsible for supporting our students, faculty, and staff members (approximately 2300 personnel total) between the hours of 0700-1700 Monday through Friday with some occasional after hour and weekend work dependent on events, seminars, or exercises that the College may be hosting. The Service Desk operates at a Tier I/II level (walk-ins and telephone calls at our Service Desk and Field Technicians for support at the user's desktops) and is the focal point for the management of IT incidents and change requests across the College. The IRD Service Desk has been realigning itself to better service our users and has begun an initial ITIL v3 implementation for incident, problem, configuration, and change managements. The software that the Service Desk uses to manage incidents is an ITIL compliant product (IT Direct). The IRD Service Desk supports the College of Distance Education's Fleet Program and will at times send technicians off-site and out of the immediate traveling area in order to meet that support. Additionally, the Customer Support Services Branch as a whole supports mobile device management (iPad, Android, and other tablets/telephones) and desktop/laptop management (software deployment, Symantec Ghost imaging, and PC lifecycle management) in coordination with our Information Security Branch, Network Branch, and Systems Administration Branch.

Information Security Branch
The Information Security Branch manages IDS/IPS systems on EDU. The branch also operates ACAS for IAVA management and scanning, McAfee HBSS for servers and workstations, and SSIM for event correlation and data analysis. Additionally, Information Security validates the remediation of IT resources managed by the other branches in the department and is the principal agent in reporting to the Navy Cyber Defense Operations Command (NCDOC) when information security incidents occur. Web content filters are used on the EDU and commercial ISP to ensure that all laws, regulations, and policies are being adhered to. Finally, the branch also is responsible for web/application penetration testing, log events across the networks, and cyber forensics when needed.

IT Business Operations Branch
The IT Business Operations Branch manages the day-to-day business operations requirements of IRD. The branch manages all IRD IT contracts and fills the COR function when required. All NWC IT procurement requests are reviewed and evaluated by branch subject matter experts and forwarded to the CIO for final approval. The branch manages the IT Hardware and Software Asset Management function for IRD and is responsible for the oversight and control all IRD owned IT resources. The branch also serves as the IRD Managers' Internal Control (MIC) program contact. The branch is responsible for creating, maintaining, and helping enforce internal IRD technical administrative policies, procedures, and standards ensuring they are consistent with Navy and DOD direction. Maintenance of DOD/DON IT related systems such as DADMS, DITPR-DON, EMASS, NAV-IDAS and PEO-IT are the responsibility of the Business Operations Branch. Finally, the IT Business Operations branch provides input to the CIO for strategic planning, project planning, budgeting, and execution of plans/projects for improvements to the IT facility throughout the NWC to enhance and support the administrative, education, war gaming, and research missions of the NWC.

College of Distance Education
IRD also supports the College of Distance Education (CDE) and provides instructional technicians and instructional system specialists for the CDE mission. CDE provides distance education through three main avenues: web-based, CD-ROM, and the Fleet Program where the Naval War College's curriculum is taught at night at various fleet centers across the country. CDE uses Blackboard for their web-based program and a combination of IT tools (Flash, compressed streaming videos, HTML, etc.) to accomplish their requirements within the web-based program and for the CD-ROM program.

Multimedia (A/V) Support Services
The Multimedia (A/V) support services group supports all of the College's academic programs, approximately 100 conferences, symposia, workshops and meetings held in Hewitt, Conolly, Spruance, Pringle, Luce, Mahan, Schonland and Evans Halls, Colbert Plaza, and Dewey Field annually for CNO, SECNAV, NWC, NWC Foundation, Navy Undersea Warfare Command and other DOD Organizations. Participants in serviced events typically include high-ranking civilians and flag and general officers. Services are provided throughout the NWC complex, which include two auditoriums, a conference center, 50+ classrooms and the President's briefing room, as well as other locations as required.

2.3 USNA ITSD

ITSD is comprised of several departments working in collaboration to implement the USNA and ITSD mission. These departments are: Cybersecurity, Information Engineering, Client Services, Systems and Communications, and Finance. ITSD strives to keep all technology current and at the forefront of technological evolution. Systems, applications, equipment, and tools, will change overtime, in some instances gradually as from one version to the next version, or drastically such as moving from one product to a different product. USNA's IT environment is dynamic and is constantly reviewed for relevance, currency, and efficiency.

The USNA IT infrastructure includes approximately 120 physical and virtual servers running Solaris, Windows Server, and Linux on a single backbone, unclassified network. There are approximately 7000 clients on the network, with several thousand others accessing externally facing web resources, such as applicants for

admission, liaison officers, etc. There is external access to a .edu network via 1Gb connection to a local educational wide-area network, and OC-12 access to DREN.

USNA currently uses Windows 2008/2012 servers for the directory services, Microsoft-server-based applications, and file-sharing environment. ERP systems are hosted on Solaris 9 servers, soon to be Solaris 11. Cloud-based Google Apps for Government provides all e-mail services and a complimentary file-sharing system. Learning management functionality is provided by Blackboard, also hosted in the cloud. Desktop office automation software is MS Office 2010. Databases are primarily Oracle, along with SQL Server. Incident management and help desk functions are automated with WebHelpDesk. Numerous academic COTS applications are used as necessary to support the mission. Web applications are managed through Cascade Server. All systems are configured to DISA STIG standards and all other applicable DoD and DoN requirements.

USNA does not currently have a SIPRNET presence. DMZ-located functions are restricted to externally-facing web applications and informational web pages.

3. REQUIREMENTS

Security requirements are at a minimum: background investigation, NACLC for IT Level II access, SSBI for IT Level I access, and up to Secret, NATO Secret, and Top Secret.

3.1 Application Development and Support

The contractor shall perform technical work on one or more of NPS'and USNA's major applications and other applications as required. Technical work may include installation, configuration, modifications, upgrading, migrating, testing, administering, and troubleshooting, for the following applications and software but may not be limited to this list:

NPS: PYTHON Student Management System, Applicant Management System (AMS), Kuali Financial System (KFS), Kuali Coues, and other Kuali software, SharePoint, Liferay, Sakai, Central Authentication System (CAS), Memorandum Accounting System (MAS), HELM (Faculty Management/Database), Academic Information Data Warehouse, Web-based Training, JIRA, Confluence, and other Atlassian software, LimeSurvey, MS Exchange, Google Apps for Government, VMware including vSphere, ESXi and View, On-Demand Desktop Streaming (ODDS), Varonis IDU Classification Framework, Server Operating Systems: Windows, OSX, Linux, Microsoft SQL, Oracle, Postgre SQL, MySQL, VBrick Video Broadcasting System, Subversion and GIT software. Support and development of other applications and software not listed anticipated as new technologies are introduced.

USNA: Admissions Information System (AIS), Midshipmen Information System (MIDS), Naval Academy Preparatory School (NAPS) Scholastic Tracking & Accountability Record (NSTAR), Enterprise Business Intelligence System (Business Objects / WebIntelligence), COTS web-based application and Oracle relational databases, Enterprise Operational Data Store and Warehouse, Google Apps for Government, VMware including vSphere, ESXi and View, On-Demand Desktop Streaming, Server Operating Systems: Windows, OSX, Linux, Microsoft SQL, Oracle, MySQL, VBrick Video Broadcasting System. Support and development of other applications and software not listed are anticipated as new technologies are introduced.

3.2 Mobile Application Development

The contractor shall develop applications for mobile devices such as but not limited to phones and tablets. The contractor shall design, develop, test, troubleshoot, maintain, and enhance mobile applications on iOS, Android, and Windows phone platforms and other systems and platforms the University and Academy may include in its inventory. Provide mobile application source code and adapt existing web applications to work on mobile platforms as well as develop applications compatible with mobile and desktop platforms.

3.3 Web Applications

The contractor shall provide development support to setup, configure, modify, test, maintain, operate, and support web sites, applications and databases to include, but not be limited to: develop, redevelop and maintain Intranet

applications single high bandwidth products such as Microsoft Silverlight and .Net framework 3.5. The contractor shall deploy and maintain Portal Services to NPS, NWC, and USNA networks, reengineer legacy applications to web based .Net applications with SQL server or other approved back-end database or Java applications with MySQL or other approved back-end database. The contractor shall provide web support for Internet, Intranet, and SIPRNET. Support shall include assisting with the development of web sites, coordination of web page development, application of required security measures, XML schema design and implementation, replication, implementation, integration of databases, deploy and maintain SharePoint Portal Server 2007 to the DMZ and SIPRNET, reengineer legacy applications to web based .Net applications with SQL server back-end databases, participate in the deployment and implementation of a new College Management System to replace a Microsoft Access based solution, and continue COTS support for applications that are used at the institutions.

3.4 Computer Network Defense (CND) Incident Response, Management, and Forensics
The Contractor shall operate, maintain, and update current computer network incident detection, response, and analysis tools and systems. The information security devices and services design and capabilities must comply with all DoD, Navy, NPS, NWC, and USNA requirements for security and Information Assurance (IA) protection.

3.4.1 Incident Response: The contractor shall install, operate, and maintain media forensics analysis tools and systems and train NPS, NWC, and USNA IA staff to use media forensics analysis tools. The contractor shall design, operate, maintain, and expand network, workstation, and server logging functions in support of incident management including development and growth of centralized log collection and analysis databases. Work shall include training NPS, NWC, and USNA Cybersecurity staff to use current and emerging incident response and analysis tools; provide assistance in investigating internal network intrusion events including on-site calls if necessary. Technician shall be physically on-site at the NPS, NWC, or USNA as prescribed in the Task Order. The contractor shall receive and analyze network alerts from various sources within the enclave and determine possible causes of such alerts, coordinate with enclave Cybersecurity staff to validate network alerts, perform analysis of log files from a variety of sources within the enclave, to include individual host logs, network traffic logs, firewall logs, and intrusion detection system logs, characterize and analyze network traffic to identify anomalous activity and potential threats to network resources. The contractor shall assist in the construction of signatures which can be implemented on Cybersecurity network tools in response to new or observed threats within the enclave, perform event correlation using information gathered from a variety of sources within the enclave to gain situational awareness and determine the effectiveness of an observed attack, notify Cybersecurity managers, Cybersecurity incident responders, and other Cybersecurity team members of suspected Cybersecurity incidents and articulate the event's history, status, and potential impact for further action, track and document CND incidents from initial detection through final resolution, perform CND incident triage to include determining scope, urgency, and potential impact; identify the specific vulnerability and make recommendations which enable expeditious remediation, correlate incident data and perform CND trend analysis and reporting, and coordinate with intelligence analysts to correlate threat assessment data.

3.4.2 Cybersecurity Protection Services: The Contractor shall provide and perform a full range of information security services support to implement, maintain and sustain all unclassified and classified information security support services required. This work shall include but not be limited to: provide information security support to setup, configure, modify, test, maintain, operate, and support information security to include, but not be limited to: firewall administration, IDS administration, policy server administration, IAVA management, DISA HBSS and ACAS management, Secure Configuration Remediation Initiative (SCRI) tool, VPN management, penetration testing, forensics research and analysis, web content filter management, security incident reporting, and vulnerability scanning and reporting, operate, maintain, and enhance current Network Access Control (NAC) functionality at NPS, NWC, and/or USNA including a Mobile Device Management (MDM) capability for government furnished and personal mobile devices. Additionally, the contractor shall provide technical support before, during, and after NPS Enterprise Firewall migration from a Cisco Systems architecture to a Fortinet architecture, create, edit, and manage approved changes to network access control lists on specialized CND systems (e.g., firewalls and intrusion prevention systems), perform system administration on specialized CND applications and systems (e.g., anti-virus, or Audit/Remediation) to include installation, configuration, maintenance, and backup/restore, implement Assessment and Authorization (A&A) formally known as Certification and

Accreditation (C&A) requirements for specialized CND systems within the enclave, and document and maintain records for them, and coordinate with the Cybersecurity Analysts to manage and administer the updating of rules and signatures (e.g., IDS/IPS, anti-virus, and content blacklists) for specialized CND applications.

3.4.3 Cybersecurity Threat Analysis Services: The Contractor shall provide a broad spectrum understanding of the threat environment at NPS, NWC, and/or USNA, specifically for the EDU and DREN, and develop and share the knowledge with NPS, NWC, and USNA to be included in a continuous monitoring framework. Work shall include but not be limited to: identify potential conflicts with implementation of any CND tools within the CND-Service Provider (SP) area of responsibility (e.g., tool/signature testing and optimization), administer CND test bed and test and evaluate new CND applications, rules/signatures, access controls, and configurations of CND-SP managed platforms, collect and analyze intrusion artifacts (e.g., source code, malware, and trojans) and use discovered data to enable mitigation of potential future CND incidents within the enclave. Additionally, perform initial, forensically sound collection of images and inspect to discern possible mitigation/remediation on enclave systems and required adjustments to current CND processes or technologies, coordinate with and provide expert technical support to enclave CND technicians to resolve CND incidents, serve as technical expert and liaison to law enforcement personnel and explain incident details, provide testimony as required, construct signatures which can be implemented on Cybersecurity network tools in response to new or observed threats within the enclave. The contractor shall perform event correlation using information gathered from a variety of sources within the enclave to gain situational awareness and determine the effectiveness of an observed attack, monitor external data sources (e.g. Cybersecurity vendor sites, Computer Emergency Response Teams, SANS, Security Focus) to maintain currency of Cybersecurity threat condition and determine which security issues may have an impact on the enclave.

3.4.4 Assessment and Authorization (A&A) Security Test and Evaluation (ST&E) Services: The Contractor shall provide services to support NPS', NWC's, and USNA's local assessment efforts required to provide the Authorizing Official (AO) Designated Representative (AODR) the necessary information to make an informed recommendation to the Navy NETWARCOM AO. This shall include but may not be limited to: validate the IA controls for applications at the Mission Assurance Category (MAC) III Sensitive, the MAC II Sensitive, and the MAC III Classified levels, document testing results of scoped technologies including documenting these results within the Navy's Enterprise Mission Assurance Support Service (eMASS), and determine and document remediation activities and mitigating controls that address all ST&E findings as documented on a Plan of Actions and Milestones (POA&M).

3.4.5 Red Team Vulnerability Analysis Services: The Contractor shall evaluate the effectiveness of NPS, NWC, and USNA Cybersecurity controls by determining reasonable attack vectors that exploit known vulnerabilities such as design penetration test scenarios consistent with management's objectives and complete and report on penetration testing of the network from both a trusted insider and an external user perspective, both from wired and wireless connections to the network(s).

3.5 Learning Management System (LMS) Service Support

The contractor shall provide consultation and administrative services for learning technology based solutions to meet NPS, NWC, and USNA LMS objectives. The Contractor shall assist in coordinating, installing, and maintaining instructional systems on .edu and commercial networks. Work may include conducting needs analysis for LMS training requirements, planning, organizing, designing sustaining, and developing training curricula, materials, and programs to meet NPS, NWC, and USNA LMS training needs, provide one-on-one and group training to instructors, generate reports and metrics to monitor and evaluate effectiveness, compliance, and relevance of the NPS, NWC, and USNA LMS Program, identify skill gaps in training and take appropriate actions to reduce learning constraints and improve existing staff and faculty skills and knowledge of the LMS, research and employ automated solutions including migrating and archiving training data.

The contractor shall respond to NPS, NWC, and USNA LMS student and faculty trouble tickets for LMS issues, including login and password retrieval, archiving, course logistics, and other end user issues and provide subject

matter expertise and knowledge transfer to NPS ITACS, NWC IRD, and USNA ITSD staff. The Contractor shall provide support to include but not be limited: develop best practices for online delivery and supplementation of courses; ensure complete and accurate data exchange between instructional systems and the institutions' Student Information System database; assist with development and launch support for electronically delivered classes (both synchronous and asynchronous), enhance online learning processes by applying the latest technologies to support teaching, learning, and research; help develop and provide recommendations for user interface, sequencing of online instruction, use of assessments, course materials, and activities.

3.6 Multimedia Educational Technology Support Services

The contractor shall provide technical recommendations for the integration of multimedia in NPS, NWC, and USNA learning spaces. The contractor shall provide technical support services to instructors, faculty and DL technologists in regards to technology and pedagogy. The contractor shall provide support to academic programs as a television camera operator, audio technician, lighting technician, and as a video technician and producer. Provides videotaping and audio taping services as well as editing and duplication services and reformatting of media. Installs, operates and maintains video and audio equipment including LCD, projectors, a CATV system, satellite up-linking and down-linking. The contractor shall provide training and documentation for implementing various multimedia applications into all aspects of the institutions' DL Programs, conduct regular classroom observations and provide technology-related feedback for improvement of DL course delivery, assess student learning techniques in consultation with the directors of the relevant educational programs.

Additionally, the contractor shall participate and contribute in informational meetings with DL instructional staff, program directors, and the technology staff to assess objectives and desired results, provide innovative technical recommendations for the integration of multimedia, virtualization, and DL instruction across campus, provide and present a range of multimedia applications to meet pedagogical goals, develop and deliver tools to publicize on-site and remote learning technology to the community of instructors, students, researchers and staff at NPS, NWC, and USNA, facilitate workshops on multimedia-related topics based on needs of the NPS, NWC, and USNA learning communities, collaborate with all information technology groups on campus and at peer institutions on new directions in technology-assisted learning, develop and implement cross-institutional technological and pedagogical initiatives, and design and implement multimedia-related strategies and technological infrastructure at NPS, NWC, and USNA.

3.7 Virtualization Services

The contractor shall provide engineering support for ongoing NHEITC virtualization initiatives such as Optimize system configuration for NHEITC's virtualization initiatives, develop recommendations to scale the virtualization Initiative for a larger audience, provide subject matter expertise on virtualization architecture and design, review proposed virtualization architecture and recommend additional optimizations as needed, provide hands-on training to Cyberinfrastructure and ET teams, plan and prepare for growth in virtual desktop demands.

The contractor shall prepare technical briefings and attend technical meetings, create and maintain documentation for users and system administrators describing the use and architecture of virtualization solutions, respond quickly to user requests for assistance and troubleshooting, test and troubleshoot end-to-end virtualization solutions, provide recommendations and implement system security measures in accordance with established IA policies, and create monthly reports that provide update on status, work completed, work in progress, short term goals, and other relevant project information.

3.8 Network and Infrastructure Maintenance

The Contractor shall design, coordinate, install, and maintain network and wireless network infrastructure for the NHEITC's networks and all associated ISP circuits. The network infrastructure design and capabilities must comply with all DoD, DoN, NHEITC requirements for security and IA (IA) protection. The Contractor shall provide and perform a full range of network infrastructure services support to implement, maintain and sustain all network infrastructure support services required, provide network infrastructure support to setup, configure, modify, test, maintain, operate, document and support networks to include installation, operation, configuration, maintenance, and repair of the following but not limited to: Switches, Routers, VPNs, ISEs (Identity Services Engine), Network Authentication systems, Permission management systems, VOIP equipment and infrastructure, Wi-Fi infrastructure, Patch panels, Copper wire for data and traditional voice services and client devices, Fiber optic installations for data

and traditional voice services and client devices, Rack installations for equipment, Cable management for networked devices, Encryption devices, Hardened Protected Distribution Systems (PDS) for SIPRNET requirements, Quality of Service (QoS) management, IPv4 & IPv6.

3.9 Network Engineering

The Contractor shall provide network engineering services and solutions support to establish, operate, and maintain NHEITC's wired and wireless networks and Cyberinfrastructure required to provide advanced network capabilities and traditional network operations on both classified and unclassified network environments. The contractor shall provide server support to setup, modify, maintain, operate, and support networks; server and system backups and restores, integration with Command authorized mobile devices through Mobile Device Manager system, implementation, server engineering, MS Exchange management, IAVA vulnerability patching, MS Active Directory management, server OS management for Windows and Linux, basic network connectivity, DNS and DHCP management, MS SQL administration, MS SharePoint administration, server application upgrades, VBrick video broadcasting systems, performance monitoring, writing and deployment of scripts, server documentation and configuration management, and managing network printer servers.

Work shall include but not be limited to:

3.9.1 Network and Server Management Operations Support: Provide onsite assistance for deployment of new technologies, optimize configuration of existing infrastructure / technologies, conduct capacity planning in support of network and security demands, conduct root cause analysis and recommend solutions to resolve network / equipment issues, install, configure, and maintain services, equipment, and devices, test and troubleshoot end-to-end network solutions and servers in various operating system and roles, support administration of network infrastructure / data center machines, monitor and improve network performance based on quantitative measures, and monitor and improve utilization of resources, both physical and virtual.

3.9.2 Virtual Infrastructure: Install, configure, troubleshoot and optimize virtual host, configure and manage virtual farm management software, orchestrate the provisioning of resources to a virtual farm, deploy virtual computer, networking, storage, and security services, create and manage self-provisioning portal for the deployment of virtualized computer, networking, storage, and security devices.

3.9.3 Training and Documentation: Develop in-depth documentation of systems, develop procedures that are correctly calibrated for the target audience to enable NPS, NWC, and USNA personnel to complete tasks, lead onsite educational workshops to expand the knowledge and skill set of network engineers and server management personnel, and review and assist with development of configuration templates, process and procedure documentation, design strategies, etc.

3.9.4 Network Infrastructure Support: The Contractor shall provide and perform a full range of network infrastructure services support to implement, maintain and sustain all unclassified and classified network infrastructure including cryptographic equipment (eg TACLANE(s), STE cards) and support services as required. The Contractor shall provide network infrastructure support to transport, setup, configure, modify, test, maintain, operate, document and support networks to include, but not be limited to: Cisco switches and routers, TACLANE(s), STEs, VPNs, NAC (Network Access Control), NetAuth (Network Authentication), Cisco permission management with TACACS+, CiscoWorks administration, patch panel management, copper wire & fiber installations for data and traditional voice services and client devices, fiber optics installations and terminations, rack installations for housing equipment, cable management for networked devices, encryption devices and hardened Protected Distribution Systems (PDS) for SIPRNET requirements, QoS management, IPv4 & IPv6 configuration & management, and configuration / change management for all networked devices.

3.10 Enterprise Architecture and Integration

The Contractor shall develop and implement Enterprise Architecture expansions or redesign and integrate multi-system solutions for the integration and automation of network administration and monitoring. The contractor shall

plan, design, and implement expansion and/or redesign of Enterprise Architecture, create specifications and requirements documentation for enterprise systems, perform cost-benefit analyses to determine whether requirements are best met by manual, software, or hardware functions; making maximum use of commercial off-the-shelf or already developed components, generate acceptance test requirements, together with the designers, test engineers, and the users, which determine that all of the high level requirements have been met, especially for the computer-human-interface, and create sketches, models, early user guides and prototypes to keep the users and the engineers constantly up to date and in agreement on the system to be provided as it is evolving.

The contractor shall conduct business analysis to determine operational objectives by studying business functions; gathering information; evaluating output requirements and formats, analyze requirements and construct workflow charts and diagrams and writing specifications, define project requirements by identifying project milestones, phases, and elements, recommend controls and improve procedures, write and maintain documentation, and prepare technical reports by collecting, analyzing, and summarizing information and trends.

The contractor shall execute integration tasks such as to specify Application Programming Interfaces (APIs) for systems used in Cyberinfrastructure and IT Operations, implement solutions to take advantage of these APIs in system administration, and document the solutions developed. The contractor shall provide training to NPS, NWC, and USNA personnel on the operation and maintenance of tools developed and automate repetitive tasks using process optimization and system integration techniques and tools.

3.11 Service Center Support Services

The contractor shall be skilled in applying customer service and customer support principles and resolve customer questions or problems concerning Information Technology systems, mobile computing systems, software and/or hardware, password, and communications systems. The contractor shall support the tier 1, 2, and 3 level customer support provided by the NHEITC. This technical support will be employed on both classified and unclassified networks. This task entails installation, troubleshooting, repair, and maintenance of NWC computer systems, connectivity, hardware, printers, and multi-function devices including: installs and configures computer systems including personal computers, microcomputers, thin and zero based clients, printers, multi-function devices and work stations, including software packages, such as client databases, spreadsheets, word processing, and communications in order to provide assistance to users; reviews malfunctioning personal computers, work stations, thin and zero based clients, printers and multi-function devices or associated hardware to isolate defective parts or determine whether inappropriate logical configurations are causing malfunctions. Repairs problem or refers problem to the higher tier.

3.11.1 Service Center Support Services Level 1: The contractor shall respond to technical trouble calls via phone, face- to-face, and email that cover the broad spectrum of services and equipment on the NHEITC networks. The contractor shall use the NPS, NWC, or USNA automated trouble ticket system, currently eHelpDesk and WebHelpDesk but transitioning to JIRA Service Desk, resolve the issue or transfer it to the appropriate team for resolution, and participate in the planning and delivery of a full range of customer support services to the organization including formal and informal information technology training and assistance to customers. The contractor shall have routine knowledge on a variety of current industry leading computer operating systems, such as Windows, Mac, Linus, iOS, Andriod, etc.; techniques, requirements and methods, seeking information from policies, directives, instructions, manuals and online information; assist with applying security and privacy requirements on user software and NHEITC network environments, work independently or collaboratively

3.11.2 Service Center Support Services Level 2: The contractor shall support technologies including but not limited to computer hardware and software, computer assisted information retrieval, data communication networks, and local area networks and technology interfaces. The contractor shall provide technical expertise on all supported automated systems used throughout the IT environment; be able to determine equipment warranty or maintenance status; ; research trends and patterns for use implementing new or improved communications methods and procedures., The contractor shall work on a variety of IT hardware in order to remove and replace defective hardware components; install network/peripheral device

interface cards, perform hardware upgrades including memory, fixed storage, and installation of network interface cards (NIC) or enhancement cards.

The contractor shall troubleshoot and correct complex software problems to include resolving conflicts between applications, hardware and/or device conflicts, and operating system faults; perform operational tests on equipment in test array or operational configuration to ensure proper operation and absence of hardware, software, device or network conflicts; keep abreast of emerging trends in IT technology ;coordinate problem resolution; assist applying security and privacy requirements on user software and the NHEITC network environments.

The contractor shall apply patches and updates and be proficient on a variety of current industry leading computer operating systems, such as Windows, Mac, Linus, iOS, Andriod, etc. NPS, NWC, and USNA network connected systems, comprehensive knowledge of various computer operating systems (Windows, Mac, Linux, iOS, Android, etc.), techniques, requirements and methods, including systems management software concepts and functions in order to install, maintain, and repair computer hardware and software, respond to, and resolve customer requests via face-to-face, email, and phone, and automate software removal and installation tasks using scripting languages.

3.12 Client Hardware & Lab Support Services

The contractor shall be skilled in applying IT principles, methods, and practices. These include IT systems development life cycle management concepts; performance monitoring principles and methods; quality assurance principles; technical documentation methods and procedures; systems security methods and procedures; analytical methods; and oral and written communication techniques. The contractor shall identify systems that are not current on updates and patches and perform remedial action, conduct system vulnerability scans using automated tools for all NPS, NWC, and/or USNA workstations, ensure anti-virus and related software packages are installed and updated on all systems, prepare and update manuals, instructions, and standard operating procedures.

The contractor shall evaluate established methods and procedures and prepare recommendations for changes in methods and practices, comprehensive knowledge of various computer operating systems (Windows, Mac, Linux, iOS, Android, etc.), techniques, requirements and methods, including systems management software concepts and functions in order to install, maintain, and repair computer hardware and software, ability to seek information from guidelines and manuals in order to research system problems and provide assistance to customers and co-workers, assist with applying security and privacy requirements on user software and NPS, NWC, and/or USNA network environments. The contractor shall support technologies including computer hardware and software, computer assisted information retrieval, imaging of Windows and Mac computer systems, remove and replace defective hardware components; install network/peripheral device interface cards, perform limited upgrade of hardware to include memory, fixed storage, and installation of network interface cards (NIC) or enhancement cards, install and configure workstation or network operating systems, and applications software on a wide range of configurable information systems devices, configure a wide variety of devices requiring diverse interfaces and device drivers in multiple operating system environments using a wide variety of hardware platforms.

The contractor shall troubleshoot and correct complex software problems to include resolving conflicts between applications, hardware and/or device conflicts, and operating system faults, perform operational tests on equipment in test array or operational configuration prior to issue or installation to ensure proper operation and absence of hardware, software, device or network conflicts, ensure the integrity and availability of all NPS, NWC, and/or USNA computer and mobile computing systems by patching and updating NPS, NWC, and/or USNA network connected systems, lab maintenance tasks such as systems preparation and integration into the lab environment, automate software removal and installation tasks using scripting languages, set up test environments, execute test plans, and report any defects or issues, develop, maintain and troubleshoot hardware image for PC and Mac, and provide patch Management.

3.13 Enterprise Information Services

The Contractor shall provide support to include but not limited to: Server and system backups and restores, server & network engineering, apply STIGS, recompose client and server images, design and deployment of scripts, server

documentation and configuration management, and managing network printer servers, provide IT Direct administration, development, and training support for IT Direct Incident Management, Problem Management, Asset Management, Change Management, Surveys, Reports, and Knowledge Base Management, develop ITIL-based businesses processes for information and process flows for incidents, problems, assets, and changes tracked in incident management system, provide web support for Internet and Intranet, on NPS, NWC, and/or USNA networks, design, develop, and implement web sites, web pages, required security measures and XML schema, provide database administration, replication, integration (extract, transform, load), migration and maintenance, design custom reports using commercially available / open source report designing software (i.e. Crystal Reports and/or Pentaho Report Designer), implement and support MS SharePoint portals, Liferay portals, Sakai LMS portals, and Google Apps for Government in support of portal projects for Internet and Intranet, support the deployment and implementation and ongoing support of the Liferay Content Management System (part of the my.nps.edu Liferay Portal) to replace a Percussion Rhythmyx based solution, and provide scripting development to automate tasks.

3.14 High Performance Computing (HPC)

The contractor shall provide support for NPS, NWC, and/or USNA HPC, including system architecture and engineering expertise to meet demand. Work shall include but not be limited to providing: troubleshooting and support of HPC systems, including routers, switches, cables, tape backup units, and disk arrays, with an emphasis on the NPS, NWC and/or USNA Supercomputer system; implementing recommendations for improved performance, including the evaluation and implementation of emerging technologies; implementing highly available storage systems using various file systems including Lustre, ZFS, and ext3/4, provided by various vendors including SuperMicro, Mellanox, Data Direct Networks and others; implementing tape archival systems to ensure retention of critical data assets.

The contractor shall implement system security hardening in accordance with established IA policies, install and maintain user applications, system patches and libraries, coordinate with other HPC team members to prioritize and accomplish assigned tasks, prepare technical briefings, create and maintain online documentation for users and system administrators describing the use and architecture of HPC system, respond to user requests for assistance: this can range from simple questions such as how to login to a machine and compile a program, to much more complex assistance such as installing specialized software, or assistance with improving the performance of a computer program, support the development and refining of scheduling policies for the batch queuing system (currently MOAB / PBS / Torque), provide support for Infiniband interconnect.

3.15 Linux System Administration

The contractor shall be responsible for analyzing, and performing work necessary to plan, design, develop, acquire, document, test, implement, integrate, maintain, and/or modify systems for solving problems or accomplishing work processes by using information technology (IT) systems such as computers, servers, embedded systems, etc. that are based on Linux operating systems. The contractor shall install and maintain software in a Linux environment, control current versions and future releases of applications software, and document the physical configuration of an information system, optimize the functionality of networks and systems and diagnose and recover failed systems identify and anticipate server performance, availability, capacity or configuration problems, and initiate corrective or preventive actions, such as increasing disk memory capacity to improve performance, reallocate resources as they become available, optimize system performance, and recommend additional components to improve overall systems performance, plan and coordinate the installation of new products or equipment, e.g. servers, network switches, monitors electrical and cooling capacity, and ensure seamless implementation, resolve installation problems, identify and mitigate security vulnerabilities and risks, maintain server integrity and availability.

The contractor shall install, configure, upgrade, and troubleshoot any hardware and software components, present formal and informal training and assistance to customers. Report, respond to, and resolve customer requests, receive, respond to, and ensure complete resolution of any help center call, document actions taken, give needed guidance or training to customers to prevent recurrences, and assist more experienced specialists in resolving very complex problems, identify and resolve a variety of conventional security issues with the ITACS IA team for security vulnerabilities, implement operations at the local activity level designed to ensure, protect, and restore IT systems, services, and capabilities, maintain a comprehensive Continuity of Operations (COOP) plan for Linux

systems for disaster recovery, and maintain a comprehensive quality assurance program for diverse platforms that cover file backup and recovery, equipment maintenance, and quality control of system processing and outputs, and monitor state-of-the-art IT developments and make recommendations on how to address trends and new technologies within the context of agency policies, plans, and management strategies, and monitor changes in Federal legislation and agency guidance, policy, regulations, and directives for potential impact on organizational policies.

3.16 Visualization Services

The contractor shall develop and apply transformational computational science capabilities in support of advances in NPS' understanding of the physical world through visualization initiatives. The contractor shall optimize system configuration for NPS visualization initiatives, develop recommendations to scale the visualization initiative for a larger audience, provide subject matter expertise on visualization architecture and design, review proposed visualization architecture and recommend additional optimizations as needed, process and interactively display real-time visual exploration of large 3D data sets with an emphasis on the efficient scalable out-of-core and parallel visual data processing of very large spatial and volumetric data sets, prepare technical briefings and attend technical meetings, create and maintain documentation for users and system administrators describing the use and architecture of visualization solutions, respond to user requests for assistance and troubleshooting, test and troubleshoot end-to-end visualization solutions, and provide recommendations and implement system security measures in accordance with established IA policies.

3.17 IT Business Operations Branch

The Contractor is responsible for the inventory, tracking, and control of all IRD owned IT assets loaned or assigned to students, faculty, and staff. These IT assets currently include, but are not limited to; laptops, iPads, cell phones, air cards, smart phones and their associated service plans. The contractor is required to use IT Direct as the official system of record for asset management. The contractor works with the Service Desk to ensure all IT assets are in a ready state for assignment or checkout by students, faculty, and staff. The Contractor is required to provide application administration and occasional training and support for IT Direct Incident Management, Problem Management, Asset Management, Change Management, Surveys, Reports, and Knowledge Base management. Support shall include the use of ITIL-based businesses processes for information and process flows for incidents, problems, assets, and changes tracked in the incident management system (IT Direct).

4.0 Deliverables

Deliverables, reports, IT services, etc shall be established on a task order basis. In addition to the deliverables established in each task order, the contractor shall submit a monthly status report to the COR, with a copy to the PCO, no later than the 10th working day of the following month that includes information as follows for all task orders awarded to date:

4.1 Task order number and type (FFP or CPFF); date of award; place of performance; total awarded dollar value; brief description of services provided; and progress and status, including any issues impacting performance and resolution of issues previously reported. The total awarded dollar value across all task orders shall also be provided.

4.2 For FFP type task orders, the proposed hours and amounts by labor classification, the proposed travel expenses, and the proposed other direct costs, and profit reflected in the final awarded price. This information shall be provided by individual task order, with totals across all FFP task orders.

4.3 For CPFF type task orders, the actual expended hours and amounts by labor classification, the actual expended travel expenses, and the actual expended other direct costs. This information shall be provided by individual task order, with totals across all CPFF task orders. Note: the Limitation of Funds and/or the Limitation of Costs clause applies at the task order level for CPFF task orders.

5.0 Security Requirements

Personnel proposed at the basic contract level shall have secret clearance at time of proposal submission and maintain that clearance for the life of the contract. Additionally, any personnel proposed at the task order level shall maintain a Secret Clearance prior to Contractor submitting a response to a task order RFP or RFQ. All individuals proposed at the task order level shall maintain a secret clearance for the life of that task order. The security requirements are in accordance with the attached DD254. Contractor Key Personnel must be U.S. Citizens.

Contractors performing on this contract are required to familiarize themselves with, and participate in, the Naval Postgraduate School's OPSEC program. Must be familiar with and comply with NAVPGSCOLINST 3432.1B, the NPS Critical Information List, DoDI 5205.2E and their applicable references. The contractor will be required to complete OPSEC and counter-intelligence training within 30 days of beginning the work, or provide proof of OPSEC and counterintelligence training completed within the previous 12 months. The contractor may not publicly release any information about developmental work or curriculum at NPS without prior written approval from the Preliminary Investigator (PI).

6.0 NMCARS 5237.102-90 Enterprise-wide Contractor Manpower Reporting Application (ECMRA)

(a) DoD contracting activities awarding or administering contracts shall incorporate the following Enterprise-wide Contractor Manpower Reporting Application (ECMRA) standard language into all contracts which include services, provided the organization that is receiving or benefiting from the contracted service is a Department of Defense organization, including reimbursable appropriated funding sources from non-DoD executive agencies where the Defense Component requiring activity is the executive agent for the function performed. The reporting requirement does not apply to situations where a Defense Component is merely a contracting agent for another executive agency. Contracted services excluded from reporting are based on Product Service Codes (PSCs). The excluded PSCs are:

(1) W, Lease/Rental of Equipment;

(2) X, Lease/Rental of Facilities;

(3) Y, Construction of Structures and Facilities;

(4) S, Utilities ONLY;

(5) V, Freight and Shipping ONLY.

(b)The standard language to be inserted is:

"The contractor shall report contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract for the [NAMED COMPONENT] via a secure data collection site. Contracted services excluded from reporting are based on Product Service Codes (PSCs). The excluded PSCs are:

(1) W, Lease/Rental of Equipment;

(2) X, Lease/Rental of Facilities;

(3) Y, Construction of Structures and Facilities;

(4) S, Utilities ONLY;

(5) V, Freight and Shipping ONLY.

The contractor is required to completely fill in all required data fields using the following web address https://doncmra.nmci.navy.mil.

Reporting inputs will be for the labor executed during the period of performance during each Government fiscal year (FY), which runs October 1 through September 30. While inputs may be reported any time during the FY, all data shall be reported no later than October 31 of each calendar year. Contractors may direct questions to the help desk, linked at https://doncmra.nmci.navy.mil.

7.0 NAVSUP 5252.204-9400 Contractor Unclassified Access to Federally Controlled Facilities, Sensitive Information, Information Technology (IT) Systems or Protected Health Information (July 2013)

Homeland Security Presidential Directive (HSPD)-12, requires government agencies to develop and implement Federal security standards for Federal employees and contractors. The Deputy Secretary of Defense Directive-Type Memorandum (DTM) 08-006 – "DoD Implementation of Homeland Security Presidential Directive – 12 (HSPD-12)" dated November 26, 2008 (or its subsequent DoD instruction) directs implementation of HSPD-12. This clause is in accordance with HSPD-12 and its implementing directives.

APPLICABILITY
This clause applies to contractor employees requiring physical access to any area of a federally controlled base, facility or activity and/or requiring access to a DoN or DoD computer/network/system to perform certain unclassified sensitive duties. This clause also applies to contractor employees who access Privacy Act and Protected Health Information, provide support associated with fiduciary duties, or perform duties that have been identified by DON as National Security Position, as advised by the command security manager. It is the responsibility of the responsible security officer of the command/facility where the work is performed to ensure compliance.

Each contractor employee providing services at a Navy Command under this contract is required to obtain a Department of Defense Common Access Card (DoD CAC). Additionally, depending on the level of computer/network access, the contract employee will require a successful investigation as detailed below.

ACCESS TO FEDERAL FACILITIES
Per HSPD-12 and implementing guidance, all contractor employees working at a federally controlled base, facility or activity under this clause will require a DoD CAC. When access to a base, facility or activity is required contractor employees shall in-process with the Navy Command's Security Manager upon arrival to the Navy Command and shall out-process prior to their departure at the completion of the individual's performance under the contract.

ACCESS TO DOD IT SYSTEMS
In accordance with SECNAV M-5510.30, contractor employees who require access to DoN or DoD networks are categorized as IT-I, IT-II, or IT-III. The IT-II level, defined in detail in SECNAV M-5510.30, includes positions which require access to information protected under the Privacy Act, to include Protected Health Information (PHI). All contractor employees under this contract who require access to Privacy Act protected information are therefore categorized no lower than IT-II. IT Levels are determined by the requiring activity's Command Information Assurance Manager. Contractor employees requiring privileged or IT-I level access, (when specified by the terms of the contract) require a Single Scope Background Investigation (SSBI) which is a higher level investigation than the National Agency Check with Law and Credit (NACLC) described below. Due to the privileged system access, a SSBI suitable for High Risk public trusts positions is required. Individuals who have access to system control, monitoring, or administration functions (e.g. system administrator, database administrator) require training and certification to Information Assurance Technical Level 1, and must be trained and certified on the Operating System or Computing Environment they are required to maintain.

Access to sensitive IT systems is contingent upon a favorably adjudicated background investigation. When access to IT systems is required for performance of the contractor employee's duties, such employees shall in-process with the Navy Command's Security Manager and Information Assurance Manager upon arrival to the

Navy command and shall out-process prior to their departure at the completion of the individual's performance under the contract. Completion and approval of a System Authorization Access Request Navy (SAAR-N) form is required for all individuals accessing Navy Information Technology resources. The decision to authorize access to a government IT system/network is inherently governmental. The contractor supervisor is not authorized to sign the SAAR-N; therefore, the government employee with knowledge of the system/network access required or the COR shall sign the SAAR-N as the "supervisor".

The SAAR-N shall be forwarded to the Navy Command's Security Manager at least 30 days prior to the individual's start date. Failure to provide the required documentation at least 30 days prior to the individual's start date may result in delaying the individual's start date.

When required to maintain access to required IT systems or networks, the contractor shall ensure that all employees requiring access complete annual Information Assurance (IA) training, and maintain a current requisite background investigation. The Contractor's Security Representative shall contact the Command Security Manager for guidance when reinvestigations are required.

INTERIM ACCESS
The Navy Command's Security Manager may authorize issuance of a DoD CAC and interim access to a DoN or DoD unclassified computer/network upon a favorable review of the investigative questionnaire and advance favorable fingerprint results. When the results of the investigation are received and a favorable determination is not made, the contractor employee working on the contract under interim access will be denied access to the computer network and this denial will not relieve the contractor of his/her responsibility to perform.

DENIAL OR TERMINATION OF ACCESS
The potential consequences of any requirement under this clause including denial or termination of physical or system access in no way relieves the contractor from the requirement to execute performance under the contract within the timeframes specified in the contract. Contractors shall plan ahead in processing their employees and subcontractor employees. The contractor shall insert this clause in all subcontracts when the subcontractor is permitted to have unclassified access to a federally controlled facility, federally-controlled information system/network and/or to government information, meaning information not authorized for public release.

CONTRACTOR'S SECURITY REPRESENTATIVE
The contractor shall designate an employee to serve as the Contractor's Security Representative. Within three work days after contract award, the contractor shall provide to the requiring activity's Security Manager and the Contracting Officer, in writing, the name, title, address and phone number for the Contractor's Security Representative. The Contractor's Security Representative shall be the primary point of contact on any security matter. The Contractor's Security Representative shall not be replaced or removed without prior notice to the Contracting Officer and Command Security Manager.

BACKGROUND INVESTIGATION REQUIREMENTS AND SECURITY APPROVAL PROCESS FOR CONTRACTORS ASSIGNED TO NATIONAL SECURITY POSITIONS OR PERFORMING SENSITIVE DUTIES
Navy security policy requires that all positions be given a sensitivity value based on level of risk factors to ensure appropriate protective measures are applied. Navy recognizes contractor employees under this contract as Non-Critical Sensitive [ADP/IT-II] when the contract scope of work require physical access to a federally controlled base, facility or activity and/or requiring access to a DoD computer/network, to perform unclassified sensitive duties. This designation is also applied to contractor employees who access Privacy Act and Protected Health Information (PHI), provide support associated with fiduciary duties, or perform duties that have been identified by DON as National Security Positions. At a minimum, each contractor employee must be a US citizen and have a favorably completed NACLC to obtain a favorable determination for assignment to a non-critical sensitive or IT-II position. The NACLC consists of a standard NAC and a FBI fingerprint check plus law enforcement checks and credit check. Each contractor employee filling a non-critical sensitive or IT-II position is required to complete:

- SF-86 Questionnaire for National Security Positions (or equivalent OPM investigative product)
- Two FD-258 Applicant Fingerprint Cards (or an electronic fingerprint submission)
- Original Signed Release Statements

Failure to provide the required documentation at least 30 days prior to the individual's start date shall result in delaying the individual's start date. Background investigations shall be reinitiated as required to ensure investigations remain current (not older than 10 years) throughout the contract performance period. The Contractor's Security Representative shall contact the Command Security Manager for guidance when reinvestigations are required.

Regardless of their duties or IT access requirements ALL contractor employees shall in-process with the Navy Command's Security Manager upon arrival to the Navy command and shall out-process prior to their departure at the completion of the individual's performance under the contract. Employees requiring IT access shall also check-in and check-out with the Navy Command's Information Assurance Manager. Completion and approval of a System Authorization Access Request Navy (SAAR-N) form is required for all individuals accessing Navy Information Technology resources. The SAAR-N shall be forwarded to the Navy Command's Security Manager at least 30 days prior to the individual's start date. Failure to provide the required documentation at least 30 days prior to the individual's start date shall result in delaying the individual's start date.

The contractor shall ensure that each contract employee requiring access to IT systems or networks complete annual Information Assurance (IA) training, and maintain a current requisite background investigation. Contractor employees shall accurately complete the required investigative forms prior to submission to the Navy Command Security Manager. The Navy Command's Security Manager will review the submitted documentation for completeness prior to submitting it to the Office of Personnel Management (OPM). Suitability/security issues identified by the Navy may render the contractor employee ineligible for the assignment. An unfavorable determination made by the Navy is final (subject to SF-86 appeal procedures) and such a determination does not relieve the contractor from meeting any contractual obligation under the contract. The Navy Command's Security Manager will forward the required forms to OPM for processing. Once the investigation is complete, the results will be forwarded by OPM to the DON Central Adjudication Facility (CAF) for a determination.

If the contractor employee already possesses a current favorably adjudicated investigation, the contractor shall submit a Visit Authorization Request (VAR) via the Joint Personnel Adjudication System (JPAS) or a hard copy VAR directly from the contractor's Security Representative. Although the contractor will take JPAS "Owning" role over the contractor employee, the Navy Command will take JPAS "Servicing" role over the contractor employee during the hiring process and for the duration of assignment under that contract. The contractor shall include the IT Position Category per SECNAV M-5510.30 for each employee designated on a VAR. The VAR requires annual renewal for the duration of the employee's performance under the contract.

BACKGROUND INVESTIGATION REQUIREMENTS AND SECURITY APPROVAL PROCESS FOR CONTRACTORS ASSIGNED TO OR PERFORMING NONSENSITIVE DUTIES

Contractor employee whose work is unclassified and non-sensitive (e.g., performing certain duties such as lawn maintenance, vendor services, etc.) and who require physical access to publicly accessible areas to perform those duties shall meet the following minimum requirements:

- Must be either a US citizen or a US permanent resident with a minimum of 3 years legal residency in the United States (as required by The Deputy Secretary of Defense DTM 08- 006 or its subsequent DoD instruction) and
- Must have a favorably completed National Agency Check with Written Inquiries (NACI) including a FBI fingerprint check prior to installation access.

To be considered for a favorable trustworthiness determination, the Contractor's Security Representative must submit for all employees each of the following:

- SF-85 Questionnaire for Non-Sensitive Positions

- Two FD-258 Applicant Fingerprint Cards (or an electronic fingerprint submission)
- Original Signed Release Statements

The contractor shall ensure each individual employee has a current favorably completed National Agency Check with Written Inquiries (NACI) or ensure successful FBI fingerprint results have been gained and investigation has been processed with OPM.

Failure to provide the required documentation at least 30 days prior to the individual's start date may result in delaying the individual's start date. In order to maintain access to required systems, the contractor shall ensure completion of annual Information Assurance (IA) training, monitor expiration of requisite background investigations, and initiate reinvestigations as required.

- Consult with your Command Security Manager and Information Assurance Manager for local policy when IT-III (non-sensitive) access is required for non-US citizens outside the United States.

SECTION L - INSTRUCTIONS, CONDITIONS AND NOTICES TO BIDDERS

The following have been modified:
INSTRUCTIONS TO OFFERORS

Section L - Instructions, Conditions and Notices to Bidders

1.0 GENERAL INSTRUCTIONS:

1.1 This solicitation is issued as a 100% Service Disabled Veteran Owned Small Business (SDVOSB) Set-Aside. The applicable North American Industry Classification System (NAICS) code is 541519 and the size standard established by the Small Business Administration is $27.5 million.

1.2 The Government contemplates award of two or more Multiple Award Indefinite-Delivery/Indefinite-Quantity type contracts with cost plus fixed fee and Firm fixed Price Task Orders resulting from this solicitation. The resultant contracts are for a Naval Higher Education Information Technology Consortium support services in accordance with the PWS provided herein. Awards will be based on a best value procurement under FAR Part 15, and consist of a one year base ordering period followed by four one-year option periods. Evaluation will extend to the option years.

1.3 Each contract will provide for the issuance of Firm Fixed Price (FFP) or Cost Plus Fixed Fee (CPFF) task orders; however, the Government intends to maximize the use of FFP task orders. The Government anticipates continuing short-term requirements originally issued on a CPFF basis will be re-competed as FFP orders to the maximum extent feasible. In accordance with FAR 37.112, the Government intends to use these contracts to acquire contractor support services, which shall not be regarded or treated as personal services. Each period of performance for all task orders shall in no event exceed one year. Task orders may contain option periods, however each option period shall in no event exceed one year.

1.4 Questions regarding this procurement must be submitted through email to the Contract Specialist at Michael.a.oliva@navy.mil. All questions submitted shall include the solicitation number in the subject line. Other methods of question submittal will not be acknowledged. The Government will make every attempt to answer all questions in a timely manner; however, questions submitted within 7 days of the posted closing date may not allow ample time to respond and offerors cannot be guaranteed a response. All questions and answers will be posted for viewing by all other potential offerors.

2.0 PROPOSAL FORMAT AND CONTENT

2.1 Offerors shall submit their proposals in the following format:

2.1.1 Offer

2.1.2 Volume I – Technical Capability

2.1.2 Volume II – Past Performance

2.1.3 Volume III – Cost

Volume Name	*Number of Copies	Page Limit
Offer **	(1) Hard Copy	Unlimited
Volume I – Technical***	(3) Hard Copies	(85) pages exclusive of resumes, letter of intents, table of contents, and table of figures.
Volume II- Past Performance	(3) Hard Copies	2 Pages exclusive of Offerors Past Performance Data –Attachment 2
Volume III- Cost	(1) Hard Copy	Unlimited

Hard copies must be mailed and received by the RFP closing date identified. HAND DELIVERED COPIES OF THE PROPOSAL WILL NOT BE ACCEPTED.

*NOTE: Hard copy is in addition to one electronic copy provided via email to michael.a.oliva@navy.mil, and shall be mailed to:

NAVSUP Fleet Logistics Center San Diego (FLCSD)
Regional Contracts Department, Code 230
ATTN: Mike Oliva, Phone #: 619-556-7201
3985 Cummings Road, Bldg 116, 3rd Floor
San Diego, CA 92136-4200

** This includes a filled out and signed copy of the original solicitation document and all amendments.
*** Volume I must not contain any price or cost information.
**** Soft copies are to be submitted on a CD mailed with the hard copy of the proposal.

2.2 Soft copies are to be submitted on a CD mailed with the hard copy of the proposal. These electronic documents shall be submitted in Adobe PDF, Microsoft Word, or Excel format. Zip files are not

allowed. Any other formats may not be accessed and may be determined as mishandled. All offers must be received by the date specified in the RFP. This posted closing date and time applies to all submissions, as well as to all parts of the proposal which are to be considered for award.

2.3 Proposals must be legible, single-spaced typewritten (on one side only) in font size “12”, and the paper size is 8 ½ x 11 inches. The font size used for graphics, charts and tables (only) may be 10 points or larger and must conform to not less than 1 inch margins. Tables, charts, and graphic depictions may be single spaced but limited to data and reference material presentation only, not textual explanations. Foldout charts or diagrams may be used within the aforementioned restrictions/page limitations. Each eight and a half by eleven foldout pages will be counted as one page (i.e., one foldout with two pages will be counted as two 8 1/2 x 11 pages). Charts or diagrams provided in foldout format must be capable of being evaluated without removal from the proposal volume. Page numbers may fall within the 1-inch margin.

2.4 All pages in each volume (hard or soft copies) shall be numbered sequentially (i.e., 1-25); pages identified above that are not included in the page limitation may be numbered differently or not at all. The Government will only evaluate that part of the proposal that complies with the instructions set forth herein. For example, if an offeror submits 87 pages, the last two pages will not be read and/or evaluated.

2.5 Clarity and completeness of the proposal are of the utmost importance. The proposal must be written in a practical, clear, and concise manner. It must use quantitative terms whenever possible and must avoid qualitative adjectives to the maximum extent possible. Proposal volumes must be internally consistent or the proposal will be considered unrealistic and may be considered unacceptable. The Government intends to award a contract without discussions as authorized by FAR 52.215-1. Any exception to the Government’s technical requirements/specifications must be resolved prior to the solicitation closing date. Offerors that take exception to the Government’s technical requirements without prior resolution with the Contracting Officer will not be considered for award**.** Alternate proposals are not authorized and will be rejected.

2.6 Notwithstanding its plan to award without discussions, the Government reserves the right to conduct discussions with offerors in the competitive range, if necessary, and to permit such offerors to revise their proposals. The Government also reserves the right to change any of the terms and conditions of the RFP by Amendment at any time prior to contract award and to allow offerors to revise their offers accordingly, as authorized by FAR 52.215-1.

2.7 The proposal must convey evidence the offeror understands all RFP and PWS requirements and their interrelationships. It must demonstrate the Offeror’s familiarity with the detailed aspects of the requirements, and clearly show that the offeror correctly interpreted all of the requirements. Offerors are cautioned against restating PWS requirements in their proposal, particularly with regard to technical requirements; and must state how all RFP and PWS requirements will be met. Statements such as "the offeror understands" and "the offeror shall/can comply", along with reference or industry references does not reflect that the offeror understands the requirements, and will likely result in a diminished evaluation rating.

2.8 Proposals shall contain only UNCLASSIFIED information. Offers shall be signed by a responsible officer representing the company who submitted the proposal. If any section of the proposal was not prepared by the individual who signs the proposal as described in the aforementioned sentence, identify the person’s name, employment capacity, the name of the person’s firm, the relationship of that firm to the offeror, and the portion of the proposal in which the person participated and their authority to bind your firm.

3.0 Volume I – Technical Proposal

3.1 Volume I of the proposal is the Technical Volume and is comprised of the Factor, and Sub-factors. It also includes the offer and signature page. No cost or pricing information shall be included in any part of the Technical Volume. The technical section of Volume I shall be divided into three clearly

labeled sections, correlating to the three sub-factors, in order. Offerors shall ensure that each sub-factor section, clearly addresses the descriptions below.

3.2 Factor I – Technical Capability

Sub-factor (1) –Technical Approach

Sub-factor (2) – Management Plan

Sub-factor (3) – Staffing Plan

3.3 Sub-factor (1) Technical Approach: To be considered further for award, offerors must :

3.3.1 Demonstrate that they are capable of fulfilling requirements of all three Naval Higher Education Information Technology Consortium (NHEIT): Naval Postgraduate School, Monterey, CA; Naval War College, Newport, RI;, and Naval Academy, Annapolis, MD; and,

3.3.2 Offerors must demonstrate they are capable of fulfilling requirements at all three geographic areas. Geographic areas of the Naval Higher Education Information Technology Consortium (NHEITC) which includes Naval Postgraduate School, Monterey, CA, Naval War College, Newport, RI, and the Naval Academy, Annapolis, MD.

3.3.3 Indicate the planned approach for meeting DoD security standards on every task order. The contractor shall provide a proposal that demonstrates the offeror meets applicable DoD facility requirements IAW the DD254.

3.3.4 The proposal shall detail the offerors experience performing work associated with an educational computing system that supports constant student, faculty and outside traffic of the network. This includes supporting distance learning, research, and administration and business systems of institutions of higher education. The proposal shall detail the offerors experience in performing key PWS areas that are unique to the .edu environment that include Learning management System (LMS) Service Support, Learning Management System (LMS) Service Support, Multimedia Educational Technology Support Services. Offerors should document how the work that ***it*** has done is similar in size and scope to the work outlined in the PWS. To maximize scoring, offerors should demonstrate its use of technology; and, should identify innovations in processes and procedures that it intends to use for this effort.

3.3.5 The technical volume shall explain the offeror's philosophy, methods, and techniques to ensure quality and consistency across the service types outlined in the PWS. The proposal shall include details of the proposed quality control plan including training, inspection system, corrective measures, and documentation, including notifying the Government COR, within one business day, when a specific PWS performance standard is not met, why the performance standard was not met, corrective action taken, and how they will prevent future occurrences.

3.4 Sub-factor (2) Management Plan:

3.4.1 The technical proposal shall contain a management plan that incorporates and demonstrates the offeror's ability to meet technical performance objectives to support the requirements of the three NHEITC member institutions. The plan shall outline the management structure to address the various elements of the PWS, the proposed technical approach and staffing plan. The plan must identify the management controls that will be put in place to assure quality and schedule accountability. The proposal shall describe the organizational freedom to identify and evaluate quality problems/discrepancies, to provide recommended solutions, and ensure corrective action is taken.

3.4.2 The proposal shall contain the offeror's approach to quality management and associated metrics gathering and reporting procedures and propose policies/procedures for managing and

directing the effort. The Offeror shall discuss a process for early identification and resolution of problems. Proposal shall address management and administrative organization. Organization/functional charts are to be used to illustrate lines of management responsibility. There must be clear identification of the chain of command and the liaison with Government.

3.5 Sub-factor (3) Staffing Plan

3.5.1 The proposal shall detail how the offeror plans to build and maintains a technically trained and experience team or workforce to satisfy task orders in support of the member institutions of varying complexity with little or no advance notice. The offer shall detail in the proposal a plan to retain the breadth and level of expertise and competence throughout the life of the contract and task orders while reducing turnover rates of personnel.

3.5.2 The proposal shall detail the approach the offeror plans to implement on meeting DoD staff investigation requirements for IT-I, IT-II, and IT-IIII level positions as defined by the PWS and the DOD. This shall include approach for placing the proper staff at the task order level in a timely fashion. The proposal shall detail the offeror's approach to recruit and retain

3.5.3 The contractor shall identify key personnel, their qualifications, and the method of retaining them throughout the life of the contract. When the offeror identifies key personnel the proposal shall contain a resume tailored to this solicitation that identifies these individuals' qualifications that supports the selection as key personnel.

4.0 Volume II– Past Performance

4.1 Past Performance shall be evaluated based on the submission of past performance data supplied by the offeror's reference/s, the Government's verification of that data (including information supplied separately by previous customers), and review of any other pertinent information. Offerors shall contact their past performance references and request that each reference complete the "Offeror's Past Performance Data" (OPPD) – Attachment 2.

4.2 Completed OPPDs shall be submitted by email directly to Michael.a.oliva@navy.mil no later than the closing date of this solicitation. The subject line of the emailed OPPD must read "SOLICITATION N00244-16-R-0009 OPPD". Offerors may submit up to three (3) OPPDs as the prime contractor; subcontractors may submit up to two (2) OPPDs.

4.3 In addition to the OPPD, offeror's shall include in Volume II, a one to two page document listing all potential references. Information to be provided is reference name, address, phone number, email address, and any other identifying information with respect to the OPPD such as Contract Number or type of work provided.

4.4 The Government shall evaluate the offeror's past performance on similar or directly-related work performed within the past three years which is similar in scope, magnitude, and complexity to that detailed in the Performance Work Statement. Past Performance shall be evaluated based on relevance and confidence (in terms of timeliness, quality, cost control, and customer satisfaction as indicated by the questionnaire). Past Performance references may include federal, state, or local Government and private contracts performed by the offeror that were similar in nature for this effort being evaluated.

4.5 Offerors may submit past performance information regarding the following: predecessor companies, key personnel who have relevant experience and subcontractors that will perform major aspects of the requirement.

4.6 Offerors may submit performance data regarding current contract performance as long as a minimum of one year of performance has been completed as of the closing date of this solicitation. Relevant past performance will be evaluated and receive scores in consonance with the evaluation scheme set forth in the RFP.

4.7 If the offeror possesses no relevant past performance, it must affirmatively state this fact in the Volume II submittal. Failure to submit OPPDs shall be considered certification that the offeror has no past performance in relevant services for the Government to evaluate.

5.0 Volume III- Cost

5.1 Offeror's cost proposal shall provide a detailed breakdown of cost data including all costs that are proposed to be reimbursed by the Government.

5.2 Contractor Labor Categories

5.2.1 Labor categories specified in the tables below may be required for performance under this contract. Labor category descriptions are provided in Attachment 1. It is recognized that Government's nomenclature may vary from that of the offeror. The cost proposal must indicate both Government and offeror nomenclature so as to clearly show consistency with labor categories submitted in the technical proposal. Failure of the offeror to provide this information in its initial offer may result in a determination that the proposal is not acceptable as it may not be susceptible to evaluation or audit.

5.2.2 Offeror that deviated from the Government labor hour's estimates shall render the proposal ineligible and shall not be considered for award. The estimated hours will be used for comparison purposes during proposal evaluation but do not necessarily reflect the number of hours that will be incurred during the performance of the Task Order. Each offeror shall allocate the labor hours as identified below for the Base Year and subsequent Option Years as follows:

NPS (Monterey, CA)						
Labor Category	**Base Year**	**Option 1**	**Option 2**	**Option 3**	**Option 4**	**Total**
Application Developer	9,600	9,600	9,600	9,600	9,600	48,000
Business Process Engineering Specialist	1,920	1,920	1,920	1,920	1,920	9,600
Communication Analyst	1,920	1,920	1,920	1,920	1,920	9,600
Data Services Developer	1,920	1,920	1,920	1,920	1,920	9,600
Database Manager/Administrator	3,840	3,840	3,840	3,840	3,840	19,200
Graphics Designer	1,920	1,920	1,920	1,920	1,920	9,600
High Performance Computing System Architect	1,920	1,920	1,920	1,920	1,920	9,600
Information Assurance Systems Specialist	9,600	9,600	9,600	9,600	9,600	48,000
Lab Services Technician	5,760	5,760	5,760	5,760	5,760	28,800
Learning Management Systems Technician	1,920	1,920	1,920	1,920	1,920	9,600
Linux Systems Administrator	1,920	1,920	1,920	1,920	1,920	9,600
Moblie Device Applicatio Developer	3,840	3,840	3,840	3,840	3,840	19,200
Network and Infrastructure Technician	3,840	3,840	3,840	3,840	3,840	19,200
Network Architect	1,920	1,920	1,920	1,920	1,920	9,600
Network Engineer	1,920	1,920	1,920	1,920	1,920	9,600
Network Systems Administrator	1,920	1,920	1,920	1,920	1,920	9,600
Service Center Specialist	5,760	5,760	5,760	5,760	5,760	28,800
Service Center Technician	5,760	5,760	5,760	5,760	5,760	28,800
Visualization Technician	1,920	1,920	1,920	1,920	1,920	9,600
Vulnerability/Threat Specialist	9,600	9,600	9,600	9,600	9,600	48,000
Web Architect	1,920	1,920	1,920	1,920	1,920	9,600
Web Content Manager	5,760	5,760	5,760	5,760	5,760	28,800
Web Designer	3,840	3,840	3,840	3,840	3,840	19,200
Total	**90,240**	**90,240**	**90,240**	**90,240**	**90,240**	**451,200**

NWC (Newport, RI)						
Labor Category	**Base Year**	**Option 1**	**Option 2**	**Option 3**	**Option 4**	**Total**
Communication Analyst	3,840	3,840	3,840	3,840	3,840	19,200
Data Services Developer	3,840	3,840	3,840	3,840	3,840	19,200
Information Assurance Systems Specialist	1,920	1,920	1,920	1,920	1,920	9,600
Learning Management Systems Technician	5,760	5,760	5,760	5,760	5,760	28,800
Network and Infrastructure Technician	3,840	3,840	3,840	3,840	3,840	19,200
Network Systems Administrator	5,760	5,760	5,760	5,760	5,760	28,800
Service Center Specialist	3,840	3,840	3,840	3,840	3,840	19,200
Service Center Technician	5,760	5,760	5,760	5,760	5,760	28,800
Total	**34,560**	**34,560**	**34,560**	**34,560**	**34,560**	**172,800**

USNA (Annapolis, MD)						
Labor Category	**Base Year**	**Option 1**	**Option 2**	**Option 3**	**Option 4**	**Total**
Application Developer	7,680	7,680	7,680	7,680	7,680	38,400
Business Process Engineering Specialist	1,920	1,920	1,920	1,920	1,920	9,600
Data Services Developer	1,920	1,920	1,920	1,920	1,920	9,600
Database Manager/Administrator	5,760	5,760	5,760	5,760	5,760	28,800
Information Assurance Systems Specialist	5,760	5,760	5,760	5,760	5,760	28,800
Lab Services Technician	11,520	11,520	11,520	11,520	11,520	57,600
Linux Systems Administrator	3,840	3,840	3,840	3,840	3,840	19,200
Moblie Device Applicatio Developer	1,920	1,920	1,920	1,920	1,920	9,600
Service Center Specialist	13,440	13,440	13,440	13,440	13,440	67,200
Service Center Technician	13,440	13,440	13,440	13,440	13,440	67,200
Vulnerability/Threat Specialist	5,760	5,760	5,760	5,760	5,760	28,800
Web Content Manager	1,920	1,920	1,920	1,920	1,920	9,600
Web Designer	1,920	1,920	1,920	1,920	1,920	9,600
Total	**76,800**	**76,800**	**76,800**	**76,800**	**76,800**	**384,000**

5.2.3 The yearly (the contractor will have to prorate these hours based on the performance periods of the CLINS in section B) level of effort for use in computing total direct labor costs is 201,600 direct labor hours. Total level of effort hours of 1,008,000 for all five years of the contract are calculated as follows:

5 yrs x 201,600 annual hours = 1,008,000

Annual level of effort Direct Labor Hours: Although actual hours performed may vary, offeror must submit a cost proposal based on this level of effort to be considered for evaluation and award.	
Labor Categories	**Hours**
Application Developer	17,280

Business Process Engineering Specialist	3,840
Communications Analyst	5,760
Data Services Developer	7,680
Database Manager/Administrator	9,600
Graphics Designer	1,920
High Performance Computing System Architect	1,920
Information Assurance Systems Specialist	17,280
Lab Services Technician	17,280
Learning Management Systems Technician	7,680
Linux Systems Administrator	5,760
Mobile Device Application Developer	5,760
Network and Infrastructure Technician	7,680
Network Architect	1,920
Network Engineer	1,920
Network Systems Administrator	7,680
Service Center Specialist	23,040
Service Center Technician	24,960
Visualization Technician	1,920
Vulnerability/Threat Specialist	15,360
Web Architect	1,920
Web Content Manager	7,680
Web Designer	5,760

5.3 Specific Requirements of Cost Proposal

5.3.1 Detailed Pricing Format. For each CLIN, offeror shall provide a detailed pricing schedule that identifies all labor categories and hours by category, direct labor rates and their application to the various labor categories, ODCs, subcontractors/consultants (if any), service centers, indirect/FCCM burden rates and their application, calculated costs, fee/profit and total pricing, by CLIN and in total for all five contract years.

5.3.2 Labor Rates. Offeror shall propose direct labor rates based on actual salaries for all key/resumed personnel. Composite/weighted average rates may be used for labor categories. Offeror shall provide detailed explanation of development of direct labor rates (e.g., based on actual salaries, labor surveys, internal labor categories, composite rates based on multiple labor categories, etc.). For those individuals proposed as current employees of the Offeror, the Offeror shall provide detailed calculation of proposed rates (e.g., composite rates) for each labor category for each CLIN. Offeror shall provide a separate schedule of internal salary rates/category rates that may be sent to DCMA/DCAA for rate verification. Offeror shall indicate if the offeror is subject to a Forward Pricing Rate Agreement for direct labor rates, and if so, shall provide a copy of the Agreement.

5.3.3 Labor Escalation. Offeror shall describe development of proposed labor escalation rate(s) (e.g., historical costs/judgment/other sources), along with the offeror's historical labor escalation rate for the previous three fiscal years.

5.3.4 Direct Labor Cost. Offeror shall provide detailed schedules calculating labor cost by labor category by year.

5.3.5 Compensation Plan. Offeror shall provide its compensation plan policy relative to salaries and fringe benefits for professional employees who will be working on the proposed contract in accordance with FAR 52.222-46, Evaluation of Compensation for Professional Employees.

5.3.6 Estimated Other Direct Costs (ODCs). To assist in proposal preparation, Government has identified annual unburdened ODC estimates to be used by offeror in preparing its cost proposal. ODCs for each performance year are identified in Section B of this solicitation. Offeror shall describe its standard burden applied to ODC, and shall apply burden to estimated ODCs pursuant to its standard burden structure.

5.3.7 Subcontracts. Offerors shall provide a copy of each subcontractor cost proposal. Offeror shall provide a schedule of proposed subcontractors and total costs proposed. Offeror will provide a schedule of subcontractor hours by labor category. Offeror will provide schedules that apply proposed subcontractor rates to proposed hours, resulting in total costs that reconcile to the proposed subcontractor amounts. For evaluation purposes only, 75% of the ODCs are for Travel and 25% are for Material.

5.3.8 Offeror shall indicate type of rate (e.g., CPFF, T&M, FFP) proposed by each subcontractor/consultant.

5.3.9 Major Subcontractors. Each subcontractor/consultant that proposes $700,000.00 or more in cost is considered to be a major subcontractor. Each major subcontractor shall provide its proposal to the contracting officer, in sealed envelope or under separate cover, in the same level of detail as required of the prime offeror, pursuant to the requirements of this section 5.3 and the below section 5.5. The subcontractor's proposal is due to the contracting officer no later than the prime offeror's proposal is due to the contracting officer.

5.3.10 Indirect Rates. Offeror shall provide a table summarizing proposed indirect rates (e.g., fringe benefits, labor overhead, material handling, general and administrative) by CLIN and by contract year, in a format that that may be sent to DCMA/DCAA for rate verification. Offeror shall provide a description of pools and bases for proposed indirect rates. Offeror shall provide calculations of composite indirect rates used for each contract year, if the offeror's fiscal year rates differ from contract year rates. Offeror shall indicate if the offeror is subject to a Forward Pricing Rate Agreement for indirect rates or DCAA provisional rates, and if so, shall provide a copy of the Agreement or DCAA provisional rate letter.

If a contractor proposes indirect rates lower than prevailing Forward Pricing Rate Agreement or DCAA-approved Provisional Billing Rates, the contractor must certify they are willing to cap these rates for the life of the contract.

5.3.11 Indirect Cost. Offeror shall provide detailed pricing schedules by contract year that clearly identify the application of indirect rates to application bases, and calculate proposed indirect costs for each indirect rate.

5.3.12 New Cost Centers. If new cost centers are developed for the proposed contract, the proposal shall provide historical data for existing cost centers for efforts similar to the requirements of this solicitation.

5.3.13 Facilities Capital Cost of Money (FCCM). If offeror elects to claim FCCM as an allowable cost, offeror must submit the calculation of proposed amounts on DD Form 1861, or equivalent, with the applicable cost of money base rates indicated, as well as percentage of total cost of money proposed by land, buildings, and equipment. Offeror shall also provide copy of the most recent completed Form CASB-CMF.

5.3.14 Fee. Offeror shall identify proposed fee rate(s) and application base(s) (e.g., 4.0% on burdened labor cost, 2.0% on burdened subcontract cost, 0.0% on burdened ODC). Offeror is

invited to submit a completed DD Form 1547 'Record of the Weighted Guidelines Application' in support of the proposed fee rate(s).

5.3.15 Historical Rates. Offeror shall provide historical direct labor rates by labor category for the three most recent completed fiscal years. For each proposed indirect/FCCM rate, offeror shall provide historical rates for the three most recent completed fiscal years, separately identifying projected vs actual rates as in the following example:

	2014	2013	2012
Projected at start of year			
Incurred at end of year			

5.3.16 Format of spreadsheets. Each offeror's cost proposal MUST be submitted in a spreadsheet format provided in Attachment 3, Sample Proposal, which includes labor categories, labor hours, direct labor rates, indirect rates, and fee. Elements contain in Attachment 3 are provided as examples only. **FORMULAS MUST BE INCLUDED WITHIN THE CELLS. COST INFORMATION SHALL NOT BE SUBMITTED IN PDF FORMAT.** The spreadsheet must list the factors used for the Base Year and each Option Year. Labor categories shall be in accordance with the tables provided in Section L. If the offeror intends on subcontracting, the aforementioned information shall be provided as well by the subcontractor.

5.3.17 Offeror shall provide a complete softcopy of its cost proposal. Softcopy shall be in Microsoft Word format for proposal narrative, and Excel format for schedules. All Excel schedules shall contain working equations and links.

5.4 Submission of Cost or Pricing Data

5.4.1 It is expected that this contract will be awarded based upon a determination that there is adequate price competition; therefore, the offeror is not required to submit or certify cost or pricing data (SF 1411) with its proposal.

5.4.2 If, after receipt of proposals, the Contracting Officer determines that adequate price competition does not exist in accordance with FAR 15.403-1, the offeror shall provide certified cost or pricing data as requested by the Contracting Officer.

5.5 Additional Required Information

5.5.1 Offeror shall provide the following additional information as an appendix/enclosure to the cost proposal. If the information is already provided elsewhere in the proposal, identify page and section number of the information's location:

5.5.1.1 DCAA office, Supervisory Auditor POC, phone number, email address, street address

5.5.1.2 DCMA office, ACO POC, phone number, email address, street address

5.5.1.3 DUNS number

5.5.1.4 CAGE Code

5.5.1.5 TAX ID

5.5.1.6 Fiscal Year (e.g., calendar year; year ending 31-July-20xx)

5.5.1.7 Brief description of company organization, parent organization if applicable, number of divisions, number of employees, annual revenues for the past three years, share of revenues provided by Govt vs Commercial, product lines, customers.

5.5.1.8 Date the accounting system was considered acceptable or approved by DCAA/DCMA

5.5.1.9 Copy of letter from DCAA/DCMA regarding acceptability of accounting system

5.5.1.10 Date the billing system was considered acceptable or approved by DCAA/DCMA

5.5.1.11 If available, a copy of the letter from DCAA/DCMA regarding acceptability of billing system

5.5.1.12 If available, the date the purchasing system was considered acceptable or approved by DCAA/DCMA

5.5.1.13 If available, a copy of the letter from DCAA/DCMA regarding acceptability of purchasing system

5.5.1.14 If available, the date of the latest financial capability audit by DCAA/DCMA

5.5.1.15 If available, a copy of the letter/report from DCAA/DCMA regarding financial capability

5.5.1.16 If available, the Date of Disclosure Statement

5.5.1.17 If available, the Date of Disclosure Statement approval by ACO

5.5.1.18 If available, a copy of the latest Forward Pricing Rate Agreement or Forward Pricing Rate Proposal

5.5.1.19 If available, a copy of latest approved Billing Rate letter

5.5.2 Offeror will provide discussion of its financial capability to perform the contract. The discussion will identify the results of any DCAA/DCMA financial capability reviews, ability to obtain financing, current financial status, etc.

5.5.3 Offeror shall demonstrate that it maintains an adequate accounting system in accordance with DFARS 252.242-7006

5.5.4 Offeror agrees to hold the prices in its offer firm for 120 calendar days from the date specified for receipt of offers.

(End of provision)

(End of Summary of Changes)