

Statement of Work

Instruction of EO3502 Telecommunications Systems Technology Electrical and Computer Engineering Department Naval Postgraduate School

1.0 Background/Introduction

The Department of Electrical and Computer Engineering at the Naval Postgraduate School (NPS) has a requirement for contractual services to deliver the course EO3502 Telecommunications Systems Technology to resident students during the Summer Quarter, Academic Year 2016.

2.0 Scope

Contractor support of a knowledgeable instructor is needed to deliver one section of EO3502. This course is a broad-based course in telecommunications systems technology for a multidisciplinary audience. The course considers analog and digital communications systems. Specific topics include amplitude and angle modulation transmission and reception; baseband and passband digital modulation; system noise; transmission lines, waveguides and antennas; fiber optics; satellite communications.

The contractor shall also update existing lecture and laboratory material to maintain consistency with the current state of the art in the field and deliver all material to the ECE department chair by the end of the Summer quarter.

3.0 Tasks

The contractor shall perform the following tasks:

- 3.1** The contractor shall update and deliver a course within the existing syllabus which articulates the learning objectives, the enabling objectives, and the grading criteria and have it reviewed by the ECE department Technical Point of Contact prior to course delivery. The contractor shall respond to student requests within 48 hours and provide written feedback on papers and projects within 5 business days.
- 3.2** The contractor shall refine and update lectures and store supporting materials on a Sakai site for student access.
- 3.3** The contractor shall assign homework readings, assignments and/or projects to support the learning environment for each course that is taught. The contractor shall periodically monitor student progress by evaluating students through quizzes and/or exams, papers or projects.
- 3.4** The contractor shall assign a final comprehensive examination or final project/paper that will be issued to the students during finals week at the end of Summer quarter AY2016.
- 3.5** The contractor shall conduct regular laboratory sessions that have a well-defined write up with instructions as to what is required of the students for a laboratory report.
- 3.6** The contractor shall prepare a mid-term student assessment and course briefing mid-way through the Summer Quarter.
- 3.7** The contractor shall provide 2 hours per week of regularly scheduled office hours during the Summer quarter of AY2016 at the Naval Postgraduate School.
- 3.8** The contractor shall submit student grade recommendations and submit them to the NPS Technical Point of Contact (POC) by the end of finals week at the end of Summer quarter AY2016.

3.9 The contractor shall conduct an overall course assessment and make suggestions for refinement

4.0 Deliverables

The contractor shall be responsible for preparing deliverables in support of the tasks identified in this SOW.

- 4.1 Syllabus and Course Materials
- 4.2 Updated Homework and Laboratory Experiments
- 4.3 Updated and developed homework
- 4.4 Final examination, project, or paper
- 4.5 Lab-write ups
- 4.6 Mid-way course assessment
- 4.7 Held office hours
- 4.8 Suggested Grades
- 4.9 Complete Course Journal (submitted via Sakai site)

Performance Work Summary

Task	What will be inspected	Acceptable Quality Level (AQL)	Method	Frequency
3.1 and 3.2	Updated syllabus and course materials on Sakai Site	Contains appropriate PowerPoint presentations to conduct class and supplemental reading materials that meet the course objectives. Course materials must be uploaded to Sakai by one week prior to delivery in the classroom	100% Inspection by the TPOC.	Inspection one week prior to delivery to students in the classroom.
3.3	Updated and any Developed homework readings, assignments and quizzes, papers, projects, and exam results.	Academic Quality	100% Inspection by the TPOC.	Due in Sakai as updated or developed
3.4	Final, comprehensive examination or final project/paper	Academic Quality Recommended grades to be submitted to TPOC. Instructor will report to the Academic Associate or the Program Officer any student that has not successfully passed an exam or project.	100% Inspection by the TPOC.	Inspection one week prior to delivery to students in the classroom.
3.5	Lab write ups	Typed and submitted into the course journal	Random Sampling	Within 1 week of delivered lab
3.6	Mid-way student assessment	Instructor will provide the TPOC with a progress report. This will include the grades from the exam and an evaluation of class at that point. Instructor will report to the Academic Associate or the Program Officer any student that has not successfully passed an exam or project.	100% Inspection	Mid-way through Summer quarter at a mutually agreed upon time.

3.7	Office hours	Instructor will post office hours and provide a list of students met with weekly.	Random Sampling	Continuous
3.8	Submission of suggested grades.	Instructor must have grades to the TPOC by an agreed upon date following the end of the Summer Quarter.	100% Inspection by TPOC	End of Course
3.9	Course Journal (in Sakai)	Complete portrayal of the course materials, lab materials, and instructor notes	100% Inspection by TPOC	End of Course

The surveillance method for the deliverables listed above will be personal observation at NPS. If performance falls below the AQL defined above, the Contracting Officer's Representative (COR) shall document the instance(s), coordinate with the Contracting Officer and advise the Contractor. The Contractor will be requested to review the documentation and provide a written response on how performance will be corrected in the future. Re-performance of any work for failure to perform in accordance with the specified AQL or task requirement shall be completed at the Contractor's own expense and at no additional cost to the Government.

5.0 Minimum Requirements

- 5.1 The contractor must be experienced at teaching graduate-level courses to U.S. and International military officers and DOD civilian students in subjects such as electrical engineering, computer engineering, electronic warfare, communications, or other closely related technical disciplines.
- 5.2 The contractor is required to have a strong academic background as demonstrated by a graduate degree in Electrical Engineering, Electrical and Computer Engineering, Electronic Warfare, or Physics.
- 5.3 The contractor must have an acceptable record of scholarly publications in the general technical area of the course. An example of an acceptable publication record is a minimum of 7 technical papers in various different journals published by the Institute of Electrical and Electronic Engineers
- 5.4 The contractor is required to be a subject matter expert in the research and design of communications systems for military applications, including ground-to-ground, ground-to-air and air-to-ground, ground-to-space and space-to-ground. The contractor should be a subject matter expert in amplitude and angle modulation transmission and reception. The contractor should be a subject matter expert in baseband and passband digital modulation. The contractor should be highly knowledgeable about subjects such as system noise, transmission lines, waveguides and antennas, fiber optics, and satellite communications.
- 5.5 The contractor must be a subject matter expert in military applications for communications systems, including ground-to-ground, ground-to-air and air-to-ground, and ground-to-space and space-to-ground.

6.0 Period of Performance

20 June 2016 through 30 September 2016.

7.0 Place of Performance

Monterey, CA campus of the Naval Postgraduate School. Specific buildings and rooms for lectures and laboratories to be assigned by NPS scheduler before start of Summer quarter. Faculty office to

be assigned in Spanagel Hall by ECE department chair. A PC connected to the NPS ERN computer network will be provided, along with an NPS email account.

8.0 Work Week and Hours of Operation:

The Contractor shall provide services during normal working hours excluding federal holidays. Normal working hours are 0730-1630, Monday through Friday, unless requirements dictate otherwise. Exceptions can be permitted by the COR upon request and at the COR’s discretion.

Work required on-site at NPS shall be performed by the Contractor, as required.

Following is a list of holidays observed by the Government.

Name of Holiday	Time of Observance
New Year’s Day	1 January
Martin Luther King Jr. Day	Third Monday in January
President's Day	Third Monday in February
Memorial Day	Last Monday in May
Independence Day	4 July
Labor Day	First Monday in September
Columbus Day	Second Monday in October
Veteran's Day	11 November
Thanksgiving Day	Fourth Thursday in November
Christmas Day	25 December

If any of the above holidays occur on a Saturday or a Sunday, then such holiday shall be observed by the Contractor in accordance with the practice as observed by the assigned Government employees at the using activity

9.0 Government Furnished Property

The government shall provide appropriate office space, supplies and equipment to perform tasks at NPS. Any Government-provided property and information shall be used for official Government business only. Any applicable documents that are authorized for use in performance of these services shall be provided, in accordance with security and contract terms and conditions.

10.0 Travel

No travel is anticipated. Any travel must be in accordance with the Joint Travel Regulations

11.0 Classification

Unclassified. Must be a US Citizen

Privacy Act Statement (no action required, leave this statement)

“Pursuant to Title 5 United States Code 552a(m)(1), the contractor and all employees of the contractor working under this contract are required to comply with the requirements of 5 U.S.C. 552a (“The Privacy Act of 1974”).”

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).

12.0 Transition Activities:

It is essential to the Government that services required under this PWS are performed without interruption. At the conclusion of any performance period, including option periods or extensions, the services provided under this PWS may be awarded to another contractor. The contractor in place shall be required to assist in the transition activities.

13.0 Non-Personal Services Statement (no action required, leave this statement)

Contractor employees performing services under this order will be controlled, directed, and supervised at all times by management personnel of the contractor. Contractor management will insure that employees properly comply with the performance work standards outlined in the SOW. Contractor employees will perform their duties independent of, and without the supervision of, any Government official or other Defense Contractor. The tasks, duties, and responsibilities set forth in the task order may not be interpreted or implemented in any manner that results in any contractor employee creating or modifying Federal policy, obligating the appropriated funds of the United States Government, overseeing the work of Federal employees, or otherwise violating the prohibitions set forth in Parts 7.5 and 37.1 of the Federal Acquisition Regulation (FAR). The Government will control access to the facility and will perform the inspection and acceptance of the completed work.

14.0 Contractor Identification (no action required, leave this statement)

In accordance with DFAR 211.106, there shall be a clear distinction between Government employees and service contractor employees. Service contractor employees shall identify themselves as contractor personnel by introducing themselves or being introduced as contractor personnel and displaying distinguishing badges or other visible identification for meetings with Government personnel. In addition, contractor personnel shall appropriately identify themselves as contractor employees in telephone conversations and in formal and informal written correspondence.

15.0 Invoice Schedule (no action required, leave this statement)

Contractor may invoice monthly in arrears.

Invoices shall be submitted once a month for services rendered and travel performed during the previous month. All invoices need to be submitted electronically via WAWF. Hard copy invoices cannot be accepted. Only one invoice may be submitted per month. Invoices must identify the invoicing period. If

charges against more than one line item have occurred during the invoicing period, all charges must be combined into one invoice. If invoicing against travel, the invoice must contain a summary detailing the charges as well as an attachment of supporting documentation. The contractor's failure to include the necessary information or a more frequent invoice submission than authorized will result in invoices being rejected.

16.0 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 NACLIC to obtain a favorable determination for assignment to a non-critical sensitive or IT-II position. The NACLIC 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 outprocess 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.