



SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS OFFEROR TO COMPLETE BLOCKS 12, 17, 23, 24, AND 30				1. REQUISITION NUMBER		PAGE 1 OF 30	
2. CONTRACT NO. HQ0034-13-A-0023		3. AWARD/EFFECTIVE DATE 17-Oct-2014		4. ORDER NUMBER 0003		5. SOLICITATION NUMBER	
7. FOR SOLICITATION INFORMATION CALL:		a. NAME				b. TELEPHONE NUMBER (No Collect Calls)	
9. ISSUED BY WHS - ACQUISITION DIRECTORATE 1155 DEFENSE PENTAGON WASHINGTON DC 20301-1155 TEL: FAX:		CODE HQ0034		10. THIS ACQUISITION IS <input checked="" type="checkbox"/> UNRESTRICTED OR <input type="checkbox"/> SET ASIDE: _____ % FOR: <input type="checkbox"/> SMALL BUSINESS <input type="checkbox"/> WOMEN-OWNED SMALL BUSINESS (WOSB) <input type="checkbox"/> HUBZONE SMALL BUSINESS <input type="checkbox"/> ECONOMICALLY DISADVANTAGED WOMEN-OWNED SMALL BUSINESS (EDWOSB) NAICS: <input type="checkbox"/> SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS <input type="checkbox"/> 8(A) SIZE STANDARD:			
11. DELIVERY FOR FOB DESTINATION UNLESS BLOCK IS MARKED <input type="checkbox"/> SEE SCHEDULE		12. DISCOUNT TERMS		13a. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700) <input type="checkbox"/>		13b. RATING	
15. DELIVER TO OSD NII JOHN ROLANDO CRYSTAL MALL 3, SUITE 6032 ARLINGTON VA 22202		CODE HQ0158		16. ADMINISTERED BY SEE ITEM 9			
17a. CONTRACTOR/OFFEROR BOOZ ALLEN HAMILTON INC. WENDY BRIDGES 8283 GREENSBORO DR MCLEAN VA 22102-3830 TELEPHONE NO. 703-304-4254		CODE 17038 FACILITY CODE		18a. PAYMENT WILL BE MADE BY DFAS-CO/SOUTH ENTITLEMENT OPERATIONS P.O. BOX 182264 COLUMBUS OH 43218-2264			
<input type="checkbox"/> 17b. CHECK IF REMITTANCE IS DIFFERENT AND PUT SUCH ADDRESS IN OFFER		18b. SUBMIT INVOICES TO ADDRESS SHOWN IN BLOCK 18a. UNLESS BLOCK BELOW IS CHECKED <input type="checkbox"/> SEE ADDENDUM					
19. ITEM NO.	20. SCHEDULE OF SUPPLIES/ SERVICES			21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
SEE SCHEDULE							
25. ACCOUNTING AND APPROPRIATION DATA See Schedule						26. TOTAL AWARD AMOUNT (For Govt. Use Only) \$6,643,292.92	
<input type="checkbox"/> 27a. SOLICITATION INCORPORATES BY REFERENCE FAR 52.212-1. 52.212-4. FAR 52.212-3. 52.212-5 ARE ATTACHED. ADDENDA <input type="checkbox"/> ARE <input type="checkbox"/> ARE NOT ATTACHED							
<input type="checkbox"/> 27b. CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4. FAR 52.212-5 IS ATTACHED. ADDENDA <input type="checkbox"/> ARE <input type="checkbox"/> ARE NOT ATTACHED							
<input checked="" type="checkbox"/> 28. CONTRACTOR IS REQUIRED TO SIGN THIS DOCUMENT AND RETURN 1 COPIES TO ISSUING OFFICE. CONTRACTOR AGREES TO FURNISH AND DELIVER ALL ITEMS SET FORTH OR OTHERWISE IDENTIFIED ABOVE AND ON ANY ADDITIONAL SHEETS SUBJECT TO THE TERMS AND CONDITIONS SPECIFIED.				<input type="checkbox"/> 29. AWARD OF CONTRACT: REF. OFFER DATED . YOUR OFFER ON SOLICITATION (BLOCK 5), INCLUDING ANY ADDITIONS OR CHANGES WHICH ARE SET FORTH HEREIN, IS ACCEPTED AS TO ITEMS:			
30a. SIGNATURE OF OFFEROR/CONTRACTOR 				31a. UNITED STATES OF AMERICA (SIGNATURE OF CONTRACTING OFFICER)  Digitally signed by BUCK.KELLIE.E.1060833962 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=WHS, cn=BUCK.KELLIE.E.1060833962 Date: 2014.10.22 17:21:56 -04'00'			
30b. NAME AND TITLE OF SIGNER (TYPE OR PRINT) Donald F. Padgett/Vice President		30c. DATE SIGNED 10/17/2014		31b. NAME OF CONTRACTING OFFICER (TYPE OR PRINT) TEL: EMAIL:		31c. DATE SIGNED	

**SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS
(CONTINUED)**

PAGE 2 OF 30

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/ SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	SEE SCHEDULE				

32a. QUANTITY IN COLUMN 21 HAS BEEN

☐ RECEIVED ☐ INSPECTED ☐ ACCEPTED, AND CONFORMS TO THE CONTRACT, EXCEPT AS NOTED: _____

32b. SIGNATURE OF AUTHORIZED GOVERNMENT
REPRESENTATIVE

32c. DATE

32d. PRINTED NAME AND TITLE OF AUTHORIZED GOVERNMENT
REPRESENTATIVE

32e. MAILING ADDRESS OF AUTHORIZED GOVERNMENT REPRESENTATIVE

32f. TELEPHONE NUMBER OF AUTHORIZED GOVERNMENT REPRESENTATIVE

32g. E-MAIL OF AUTHORIZED GOVERNMENT REPRESENTATIVE

33. SHIP NUMBER

34. VOUCHER NUMBER

35. AMOUNT VERIFIED
CORRECT FOR

36. PAYMENT

37. CHECK NUMBER

☐ PARTIAL ☐ FINAL

☐ COMPLETE ☐ PARTIAL ☐ FINAL

38. S/R ACCOUNT NUMBER

39. S/R VOUCHER NUMBER

40. PAID BY

41a. I CERTIFY THIS ACCOUNT IS CORRECT AND PROPER FOR PAYMENT

42a. RECEIVED BY *(Print)*

41b. SIGNATURE AND TITLE OF CERTIFYING OFFICER

41c. DATE

42b. RECEIVED AT *(Location)*

42c. DATE REC'D *(YY/MM/DD)*

42d. TOTAL CONTAINERS

Section SF 1449 - CONTINUATION SHEET

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0001	Cyber Security Support FFP The contractor shall provide technical support services for the DoD CIO Cybersecurity & Information Assurance Support Program IAW with the requirements as delineated in the attached TWS.	12	Months	(b)(4)	(b)(4)
NET AMT					(b)(4)
000101	Informational SubCLIN for CLIN 0001 FFP Informational SubCLIN for CLIN 0001				\$0.00
NET AMT					\$0.00
ACRN AA					(b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
000102					\$0.00

Informational SubCLIN for CLIN 0001
FFP

Informational SubCLIN for CLIN 0001

NET AMT	\$0.00
---------	--------

ACRN AB

(b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
000103					\$0.00

Informational SubCLIN for CLIN 0001
FFP

Informational SubCLIN for CLIN 0001

NET AMT	\$0.00
---------	--------

ACRN AC

(b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
000104					\$0.00

Informational SubCLIN for CLIN 0001
FFP

Informational SubCLIN for CLIN 0001

NET AMT	\$0.00
---------	--------

ACRN AD

(b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0002	Travel	25,000	Cost		\$25,000.00
	COST				
	Travel when pre-approved by the Government. Travel for this contract must be in accordance with FAR 31.205-46, "Travel Costs" and the JTR.				
				ESTIMATED COST	\$25,000.00
	ACRN AD				\$25,000.00

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0003	ODCs	9,000	Cost		\$9,000.00
	COST				
	Contractor shall provide support for Government designated meetings and conferences in accordance with Paragraph 2.1.3 of the TWS.				
				ESTIMATED COST	\$9,000.00
	ACRN AD				\$9,000.00

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
1001	Cyber Security Support	12	Months	(b)(4)	(b)(4)
OPTION	FFP				
	The contractor shall provide technical support services for the DoD CIO Cybersecurity & Information Assurance Support Program IAW with the requirements as delineated in the attached TWS.				

NET AMT

(b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
1002		25,000	Cost		\$25,000.00
OPTION	Travel				
	COST				

Travel when pre-approved by the Government. Travel for this contract must be in accordance with FAR 31.205-46, "Travel Costs" and the JTR.

ESTIMATED COST	\$25,000.00
----------------	-------------

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
1003		9,000	Cost		\$9,000.00
OPTION	ODCs				
	COST				

Contractor shall provide support for Government designated meetings and conferences in accordance with Paragraph 2.1.3 of the TWS.

NET AMT

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
2001 OPTION	Cyber Security Support FFP The contractor shall provide technical support services for the DoD CIO Cybersecurity & Information Assurance Support Program IAW with the requirements as delineated in the attached TWS.	12	Months	(b)(4)	(b)(4)

NET AMT

(b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
2002 OPTION	Travel COST Travel when pre-approved by the Government. Travel for this contract must be in accordance with FAR 31.205-46, "Travel Costs" and the JTR.	25,000	Cost		\$25,000.00

ESTIMATED COST

\$25,000.00

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
2003 OPTION	ODCs COST Contractor shall provide support for Government designated meetings and conferences in accordance with Paragraph 2.1.3 of the TWS.	9,000	Cost		\$9,000.00

ESTIMATED COST

\$9,000.00

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
3001		12	Months	(b)(4)	(b)(4)
OPTION	Cyber Security Support FFP The contractor shall provide technical support services for the DoD CIO Cybersecurity & Information Assurance Support Program IAW with the requirements as delineated in the attached TWS.				
NET AMT					(b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
3002		25,000	Cost		\$25,000.00
OPTION	Travel COST Travel when pre-approved by the Government. Travel for this contract must be in accordance with FAR 31.205-46, "Travel Costs" and the JTR.				
ESTIMATED COST					\$25,000.00

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
3003		9,000	Cost		\$9,000.00
OPTION	ODCs COST Contractor shall provide support for Government designated meetings and conferences in accordance with Paragraph 2.1.3 of the TWS.				
ESTIMATED COST					\$9,000.00

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
4001 OPTION	Cyber Security Support FFP The contractor shall provide technical support services for the DoD CIO Cybersecurity & Information Assurance Support Program IAW with the requirements as delineated in the attached TWS.	12	Months	(b)(4)	(b)(4)
NET AMT					(b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
4002 OPTION	Travel COST Travel when pre-approved by the Government. Travel for this contract must be in accordance with FAR 31.205-46, "Travel Costs" and the JTR.	25,000	Cost		\$25,000.00
ESTIMATED COST					\$25,000.00

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
4003 OPTION	ODCs COST Contractor shall provide support for Government designated meetings and conferences in accordance with Paragraph 2.1.3 of the TWS.	9,000	Cost		\$9,000.00
ESTIMATED COST					\$9,000.00

PWS**PERFORMANCE BASED TASK WORK STATEMENT (TWS)****for**

Department of Defense (DoD) Chief Information Officer (CIO)
DoD CIO Cybersecurity and Information Assurance Support Program

1.0 INTRODUCTION

1.1 BACKGROUND: The DoD CIO is the Principal Staff Assistant (PSA) and advisor to the Secretary and Deputy Secretary of Defense for Information Technology (IT), including National Security Systems (NSS) and Information Resources Management (IRM) matters. The DoD CIO is responsible for all matters relating to information and the DoD information environment including C2; communications; radio frequency spectrum; network operations; information systems; Information Assurance (IA); defensive cyber security; and Positioning, Navigation, and Timing (PNT).

The Deputy CIO (DCIO) for Cybersecurity (CS) is the Department's Senior Information Security Officer (SISO). As the DCIO(CS) he responsible for ensuring the Department has a well-defined and well executed cyber security program, and is responsible for coordinating cyber security standards, policies and procedures with other federal agencies, coalition partners, and industry.

1.2 SCOPE: The scope of this TWS is to fulfill DoD CIO requirements for technical support services for the DoD CIO Cybersecurity & Information Assurance Support Program. In addition, the objective of this TWS is to fulfill the DoD CIO requirement for comprehensive cybersecurity services in areas such as cybersecurity strategy, cybersecurity policy development, defense-wide information assurance, identity assurance, communications security (COMSEC), defense industrial base cyber security, trusted mission systems and networks analysis, architectures, standards, and day-to-day security and administration. The work will primarily support programs managed by the CS DCIO with emphasis on the following thrust areas:

- Investment & Data Collection
- Cybersecurity Implementation & Integration
- Cybersecurity Technology
- Cyber Innovation, Risk Measures and Mitigation, and Workforce Development
- IA/Cybersecurity Plans and Programs, Risk Management Oversight, and Federal Information Systems Management Act (FISMA) Support

To meet this requirement, the contractor shall provide the required special knowledge and skills not otherwise available within the DoD CIO organization. The performance requirements for this task order are delineated in the following three increments – general performance requirements, specific performance requirements, and special performance requirements.

2.0 PERFORMANCE REQUIREMENTS

2.1 GENERAL PERFORMANCE REQUIREMENTS

2.1.1 The majority of the work associated with this task order will be performed in accredited Government Sensitive Compartmented Information Facilities (SCIFs). All contractor personnel will primarily perform the performance requirements delineated in this task order inside such SCIFs on an unescorted basis. In the performance of the scope of work, contractors will come into contact with classified information concerning, or information that is derived from, intelligence sources, methods, or analytical processes. Such materials must be handled within formal access control systems requiring that all contractor personnel working on this task order hold a current Top Secret Clearance with SCI access.

2.1.2 The contractor shall provide program management support to include productivity and management methods administration, quality assurance, configuration management, work breakdown structure maintenance and human engineering services for this task order; and provide centralized administrative support and documentation. The contractor shall develop a written task order work plan, describing the approach, organizational resources, and management controls to be employed to meet the task cost, performance and schedule requirements. The contractor shall provide a monthly task status report monitoring quality assurance, configuration management, manning, and security. The contractor shall support all In Process Reviews (IPRs).

2.1.3 The contractor shall support meetings, seminars, symposia, workshops and working groups, conferences (includes teleconferences and video conferences), off-sites, Integrated Product Team (IPT) sessions and forums to include processing requests, scheduling, arranging for facilities, preparing materials, and recording and producing minutes as well as reports and oral briefings. The contractor shall provide pre-event planning, on-site coordination, and post-event activities support. Pre-event planning will include site selection, development, and distribution of announcements, agenda and event materials, and registration. On-site coordination will include attendee check-in, security problem resolution, document control, and host facility coordination. Post-event efforts shall include developing and mailing conference proceedings and generating a lessons learned report. The contractor shall have the ability to provide conference facilities in the Washington D.C. Metropolitan area.

2.2 SPECIFIC PERFORMANCE REQUIREMENTS

Recognizing that information is a strategic asset, the Department is committed to an ambitious effort to realign and restructure how information technology networks and systems are constructed, operated, and defended. This effort will result in a "Joint Information Environment" (JIE) that will provide better access to information, improve our ability to defend the networks and the data, and enable us to be more responsive to constantly changing technological and operational factors, including amplified cyber threats from our adversaries. The JIE will be a secure joint information environment, comprised of shared information technology (IT) infrastructure, enterprise services, and a single security architecture to achieve full spectrum superiority, improve mission effectiveness, increase security and realize IT efficiencies. JIE will be operated and managed per the Unified Command Plan (UCP) using enforceable standards, specifications, and common tactics, techniques, and procedures (TTPs). The contractor shall:

Investment & Data Collection Section

Task 2.2.1 Support JIE program planning, budgeting and resource processes and review plans, budget information and spending to ensure visibility, adequate resourcing, and accountability.

Task 2.2.2 Support the DOD CIO's efforts to ensure component compliance with program and budget guidance, including the annual DoD CIO Capability Planning Guidance.

Task 2.2.3 Support the DOD CIO's review and assessment of resourcing and funding strategies for IT capabilities (e.g. enterprise services). Provide resourcing analysis and strategies suitable for decision-making by senior OSD leadership.

Task 2.2.4 Support the development of a JIE Independent Budget Estimate (IBE). The IBE shall provide replicable and defensible data on how much the Department is planning/programming/budgeting for JIE. Support the analysis of DOD component budget estimates against the IBE to determine estimate gaps, risks, and impact.

Task 2.2.5 Support the JIE budget review to close gaps minimizing risks and impacts.

Task 2.2.6 Support the development of a JIE Cost Model. Support the identification of processes to improve visibility into IT investment activities, budgets, and spending across all IT portfolios in DoD. Develop strategies and sponsor activities to meet those needs. Support the program or portfolio reviews for the DoD IT infrastructure and cybersecurity portfolios or investments.

Task 2.2.7 Support the Standard and Native Programming - Defense-wide IA Program (SNaP-DIAP) authoritative IA database requirements in accounting for major projects; providing programmatic information for the President's Budget, congressional reports, briefings and testimony, and Congressional Justification Books (CJBs); publishing and/or maintaining the DoD Strategy for Defending Networks, Systems and Data; and facilitating the Planning, Programming, Budgeting and Execution processes (PPBE).

Cybersecurity Implementation & Integration Section

Task 2.2.8 Support IA and cyber security strategic planning and analysis to include IA Strategic Plan and Information Operations (IO) Roadmap activities geared to DoD strategic leadership and management. The contractor shall support the integrated management of the IA Strategic Plan related objectives, goals and accomplishments; IA policy and strategic direction; IA strategic initiatives; enabled Net-Centric operations; domestic and coalition cyber partnerships; and collaborations regarding secure and resilient network architectures.

Task 2.2.9 Support the policy development, and the related engineering and architectural initiatives, to further information assurance over DoD networks in accordance with guidance, and shall support the Department's commitment to evolve a Joint Information Environment (JIE) framework of IT capabilities and processes to further the evolution and achievement of a secure, joint information environment comprised of shared IT infrastructure, enterprise services, and a single security architecture.

Task 2.2.10 Support international outreach and awareness activities relating to Information Assurance (IA), Computer Network Defense (CND) and Cyber Security, and International IA Program (IIAP) efforts to promote regional cooperation, information sharing, and interoperability initiatives aligned to greater national and DoD policy objectives. The contractor shall also support collaborations with the Joint Staff, applicable Combatant Commands, and other agencies for coordinated policy development and international IA/CND engagement.

Task 2.2.11 Provide technical and analytical research support related to IA management methodologies and associated services. The contractor shall support the integration of these methodologies and associated services into the Knowledge Service (KS) such that the deployed KS will map IA policy to actionable IA metrics, emphasizing certification and accreditation and related IA program management metrics. The contractor shall support efforts to ensure IA metrics track with standard validation methods and mechanisms associated with IA controls, therefore ensuring the process can be easily scaled to the DoD enterprise, to include essential reporting mechanisms.

Task 2.2.12 Provide support for establishing an integrated enterprise-wide decision structure for cybersecurity risk management (the RMF) that aligns with applicable guidance and policy -- DoD Instructions, NIST Publications, and Committee on National Security Systems (CNSS) Instructions. This involves supporting needed transformation processes from DIACAP to the RMF, and the applicable analytical support to evaluate the decisions of the RMF TAG as they relate to the Knowledge Service functionality, and analysis and research support relating to deployment of RMF parameters for enterprise, organizational level, classified, and prototype versions of the tool. Requirements include organizational change management, training, site evaluation, installation operations knowledge, system configuration expertise and associated services. Support shall be performed in a seamless manner in order to synergize the virtual IA policy and KS controls configuration management capability with the IA controls to generate real time automated policy.

Cybersecurity Technology Section

Task 2.2.13 Provide technical analysis and database administration support required for the development, tracking, management, assessment of the full spectrum of DIB cyber security requirements (includes DoD, other Government agencies, and DIB partner requirements), and support the analysis of technical strategy, planning and policy studies. The contractor shall provide research, analysis and development support for leap ahead technology pilots, test beds, ranges and demonstrations, technical configuration, standards development, development of tools and applications, systems integration and interoperability, resource management, and coordination actions to aid in the formulation of technologies, policies, plans and guidance for the DIB CS/IA program, the development of analytic reports and trend analyses, as well as support for the analysis and evaluation of methods for performing continuous workflow processes improvements, and for routine internal operations and business functions.

Task 2.2.14 Support interaction with DIB Partner Chief Executive Officers, Program Managers, Chief Information Officers, Chief Information Security Officers, as well as with other DoD components and Government agencies. Tasks also include providing support in the areas of planning, data collection, populating databases, technical program analysis and database administration required to track, analyze and evaluate the full spectrum of cyber security requirements, tracking congressional actions, presentations, reporting, developing and implementing

the DIB CS/IA action plan, and providing full technology development and commercialization cycle support required to execute departmental responsibilities for the DIB CS/IA program.

Task 2.2.15 Support interface requirements and coordination efforts involving the DIB CS/IA program office and DIB Partners, and support database planning and coordination to ensure updated contact information with an expanding numbers of DIB Partners, and support for reviews of management data from DoD and DIB stakeholders in order to implement operational options. This shall include support for the management and integration of data from various sources for purposes of analyzing operational environments, employing state of the art scheduling software and collaborations tools, as well as for developing analytic reports and trend analyses.

Task 2.2.16 Provide support in the areas of operations assessments, service area management, technical reports (includes trip reports) and improvements (includes system configuration) recommendations, and provide the planning, execution and oversight of the DIB CS/IA action plan, which establishes activity project plans, measures performance and assesses impacts and issues related to DIB CS/IA task execution. Support the coordination and management of correspondence, site visits, working groups, and the associated functions to enable government technology initiatives, and provide technical development support required for management oversight of the DIB CS/IA action plan.

Task 2.2.17 Support Defense Cyber Crime Center (DC3) oversight and DIB CS/IA planning, programming, budgeting and execution (PPBE) requirements, support the Department of Homeland Security (DHS) interface and coordination support, provide DIB CS/IA program office and interagency interface and coordination support, support development and implementation of interagency agreements, to include agreements with DHS relating to cyber information threat sharing with other critical infrastructure sectors, and support the development and implementation of memorandums of understanding (MOUs), to include one with the Department of Energy to share cyber security threat information; and infrastructure sectors.

Task 2.2.18 Support the development and expansion of DIB CS/IA activities to include engagements with international partners, provide technical, analytic and programmatic support for international strategy and operation integration policy, the development, formulation and review of national level policy guidance, oversight and decision-making activities, support the review of policies and the development of DIB CS/IA policy guidance, requirements and program recommendations as well as supporting the assessment of risks and program performance, for draft plans, reports, presentations, correspondence, and other documents in support of technical analysis and policy development, and support for the development of strategic DIB CS/IA program documents.

Cyber Innovation, Risk Measures and Mitigation, and Workforce Development Section

Task 2.2.19 Support DoD CIO's development of options to implement DoD's Cyber Education efforts, to better leverage resources and achieve objectives. Focus includes: oversight of the National Initiative for Cyber Education (NICE); DoD enterprise cyber/IT training and education efforts; senior-leader curriculum development and delivery; outreach to the private sector; and partnerships with inter-agency and international partners. Support research and development of advice on policies, plans, and processes regarding the cyber workforce, analysis of their effects on cyber education, and coordination of results. Include research into CIO's involvement in the Defense Strategy for Operations in Cyberspace and General Cyber/IT, past strategy, policy, operations, force structure and manpower studies, as well as Services and Defense Agency perspectives. Research shall cover national and inter-agency efforts related to establishing an effective cyber cadre/human capital plan and strategy, the makeup and shaping of how the Cyber Strategy, Policy, and Cyber Cadre may impact how the DoD meets its transformational cyber security roles and responsibilities, and the analysis and development of recommendations on how best to provide cyber security training and education in cybersecurity courses for the DoD.

Task 2.2.20 Support implementing the Defense Strategy for Operating in Cyberspace (DSOC) directed Private Sector Partnership effort, including outreach to small and medium companies, leveraging existing outreach efforts, identifying and creating new venues as appropriate, creation of an innovation framework, establishment of metrics, and coordination of intra-DoD and interagency efforts. Includes research and analysis of DoD and Inter-Agency cyber innovation activities, making recommendations on concepts for DoD and CIO roles and activities, as well as

making recommendations for their implementation. Assist coordination among various offices within DoD and other outside public-private entities to help implement the CIO led DoD strategy, and provide guidance for developing technology insertions plans for the new and innovative cyber security technologies in the cyber environment across the DoD.

Task 2.2.21 Provide support to the DCIO (CS) for the Information Assurance Scholarship Program (IASP). This includes coordination of regular meetings with the Steering Committee in the development of communication materials for committee members, including meeting minutes and updates regarding program administration issues; in providing assistance to implement the IASP marketing campaign to include representing the IASP at conference exhibitions as needed; reviewing all documentation associated with the IASP for completeness, accuracy, and readability; reviewing capacity building proposals submitted by selected universities designated as Centers of Academic Excellence (CAE) in IA for relevance to DoD priorities; and providing necessary support during educational site visits to CAEs.

Task 2.2.22 Support development of, needed revisions to, and staffing of, relevant DoD Directives, Instructions, and other policy issuances that support the on-going development and maintenance of relevant IA/Cybersecurity Workforce Strategy documents, and support for the completion of the multi-step IA/cybersecurity professional certification project to include the development of a list of principal security-related job functions of positions within DoD and the development of a list of skills and knowledge deemed necessary to perform each of the job functions at one or more levels. Support mapping existing professional IA certification programs to DoD IA job functions to support policy implementation effort; support Line of Business (LOB) Tier I and Tier II liaison support to CS DCIO participation in the Office of Management and Budget (OMB)/Department of Homeland Security (DHS) LOB updates to training products to meet requirements for the DoD Tier I Awareness and Tier II Specialized IA Training; and support IA Workforce Improvement Program (WIP) to include the WIP Advisory Council (WIPAC) and its working groups to include the applicable policy implementation.

Task 2.2.23 Support IA/cybersecurity workforce-related reporting, including FISMA, and responses to inquiries from Congress and other appropriate DoD elements, by coordinating the integration of IA workforce data. This includes activities external to the CS DCIO in partnership with DHS, National Institute of Standards and Technology (NIST), the State Department, allies, training vendors and certification providers in support of cybersecurity training, education, awareness, and workforce activities; and support CS DCIO liaison responsibilities for the National Initiative for Cyber Education (NICE) initiative and the Cybersecurity Workforce Framework.

IA/Cybersecurity Plans and Programs, Risk Management Oversight, and Federal Information Systems Management Act (FISMA) Support Section

Task 2.2.24 Support the management of DoD FISMA Integrated Process Teams (IPT) and related working groups to include the management of administrative functions for the meetings to minutes, attendance lists, and general logistics functions associated with group meetings; and support the FISMA team on behalf of the CS DCIO managing and analyzing data feeds from the CC/S/As used to develop the FISMA report in accordance with the Office of Management and Budget (OMB) Congressional reporting guidance.

Task 2.2.25 Formulate and coordinate DoD responses to Presidential and National Security Systems direction for Insider Threat initiatives on behalf of the CS DCIO; develop DoD Insider Threat program IA details and integrate overall actions with USD (Intelligence) and ASD (Homeland Defense and American Security affairs)(HD&ASA); formulate and facilitate the implementation of DoD Insider Threat initiatives with assessments of requirements and recommendations for implementation with the USCYBERCOMMAND, NSA, and other Intelligence community entities; coordinate CS DCIO actions with the appropriate IA personnel from the Department's Combatant Commands/Services/Agencies (CC/S/A) as required; and support development of associated Insider Threat papers, reports, and presentations.

Task 2.2.26 Provide oversight of the DoD Ports, Protocols, and Services Management (PPSM) Program to include policy development; support the PPSM chair with the PPSM Configuration Control Board (CCB) as required; and provide oversight, capability requirements, and resources management for cybersecurity capabilities to

include support for the IA & Computer Network Defense (CND) Enterprise Solutions Steering Group (ESSG) meetings, for Program Objective Memorandum (POM) initiatives as required, and with needed engagement with Major Defense Acquisition Program (MDAP) and Major Automated Information System (MAIS) program offices to ensure that IA strategies and activities are adequate.

Task 2.2.27 Support operationalizing the DoD Strategy for Defending Networks, Systems, and Data (DDNSD), including establishing objectives, metrics, and monitoring tasks.

Task 2.2.28 Provide program management support to the Risk Management Oversight team in the development and implementation of IA-related technology and acquisition guidance, improving the integration of IA into the defense acquisition process, and analyzing and implementing IA technology. This will include providing expertise and support for CS DCIO interests at MDAP and MAIS integrating Integrated Process Teams (IPT) and working-level IPTs, with OUSD (AT&L), DDR&E, DARPA, etc. in integrating technology into the DoD IA program, and in reviews and analyses of MDAP and MAIS IA strategies, Program Protection Plans (PPP), acquisition strategies, Test and Evaluation Master Plans (TEMP), System Security Plans (SSPs), and assessments as to their adequacy.

Task 2.2.29 Maintain liaison with OUSD (AT&L), Component CIO offices, the IA community on emerging IA issues, and with the appropriate IA personnel from the Department's Combatant Commands / Services / Agencies (CC/S/A) as required. Support the preparation of meeting materials (schedules, agendas, meeting minutes, and briefing materials) for, and facilitate working group meetings associated with, integrating IA technology and IA into the acquisition process.

Task 2.2.30 Support development, implementation, and execution of the DoD Risk Management Framework (RMF) for Information Technology; the integration of Cloud, Mobility, Continuous Monitoring, and other major initiatives into the RMF; the development and maintenance of appropriate DoD policy and guidance concerning IA as it relates to cybersecurity risk management and DoD acquisition.

Task 2.2.31 Support development and delivery of CS DCIO-sponsored IA outreach efforts, such as the annual IA workshop, conferences, and symposiums.

2.3 SPECIAL PERFORMANCE REQUIREMENTS

2.3.1 Contractor personnel will primarily work on-site within Government facilities such as in the Pentagon, Mark Center, Crystal City, Rosslyn, Fort Belvoir, and surrounding metropolitan Washington, D.C. locations. The Government will furnish the necessary workspace for the contractor staff to provide the support outlined in this TWS to include desk space, telephones, computer equipment to include access to the Unclassified but Sensitive Internet Protocol Router Network [formerly called the Non-Classified Internet Protocol Router Network (NIPRNet)] and Secret Internet Protocol Router Network (SIPRNet), and other items necessary to perform in a normal office environment. The Government will neither provide mobile communications devices such as smart phones to Contractor employees, nor reimburse Contractors for purchase of mobile communications devices through any issued contract/task order.

2.3.2 Contractor will ensure that contract employees that require routine access to Government facilities during their performance in-process and out-process through the DoD CIO Security Office in Room 3B1056, Pentagon (e-mail address is: osd.pentagon.dod-cio.mbx.dod-cio-security@mail.mil). Contractor personnel working on this task order may be issued a Pentagon badge and/or Common Access Card (CAC) for access to the Pentagon building, allowing unescorted access. Other contractor personnel will be issued other Government-issued badges to allow unescorted access to other Government buildings. Contractor personnel shall complete the appropriate security paperwork and comply with associated policies. It is imperative that all contractor personnel understand that these Government-issued badges that allow unescorted access to Government buildings remain Government property and that they shall be returned to the office that issued the badge immediately upon the decision, or notification, that he/she is no longer working on this task order. For the Pentagon, all Pentagon badges and CAC cards must be returned to the DoD CIO Security Office in Room 3B1056, Pentagon. Contractor personnel may be required to access data and information

proprietary to the Government while performing under this task order. Contractor personnel may also have information of such a nature that its dissemination or use, other than in performance of this task order would be adverse to the interest of the Government or others. The contractor shall not divulge or release data or information developed or obtained in performance of this task order except to authorized Government personnel, or upon written approval of the Contracting Officer's Representative (COR). The contractor shall not use, disclose, or reproduce proprietary data, other than as required in the performance of this task order. The limitations above do not apply to data or information that has been made public by the Government. In the course of performance pursuant to this task order, the contractor may require access to non-public information such as Planning, Programming, Budgeting, and Execution (PPBE) information. In the event that the Contractor requires access to PPBE information while performing duties under this task order, the contractor shall agree that each of its employees and others performing work under this task order shall sign the Non-Disclosure Agreement provided as part of the solicitation. All products produced and their associated work papers are to be considered the property of the Government. Prior to assigning Contractor employees that require access to Government facilities to this task order, the Contractor's Facility Security Officer FSO shall submit Personnel (Security) Clearance (PCL) validation through use of a Visit Authorization Request (VAR) for each employee, to the DoD CIO Security Office in Rm. 3B1056, Pentagon, in accordance with DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM).

3.0 SCHEDULE AND PERFORMANCE

3.1 SCHEDULE OF DELIVERABLES

All deliverables must meet professional standards and meet the requirements set forth under criteria for acceptance. The Contractor shall be responsible for delivering all end items specified. The following items are deliverables that fall within the scope of this task and are illustrative of the type of work the Government expects to order:

Deliverable	Schedule	Submit to
Initial Draft Written Task Order Work Plan – task 2.1.2 (includes contractor Staffing Plan) delineated by the following sections: Investment & Data Collection Cybersecurity Implementation & Integration, Cybersecurity Technology, Cyber Innovation, Risk Measures, & IA/Cybersecurity Plans and Programs, Risk Management Oversight, and Federal Information Systems Management Act (FISMA).	Within 10 days of Task Order Award.	BPA Manager, COR, & each Government Section Lead.
Final Written Task Order Work Plan task 2.1.2 (includes final contractor Staffing Plan) delineated by the following sections: Investment & Data Collection Cybersecurity Implementation & Integration, Cybersecurity Technology, Cyber Innovation, Risk Measures, & IA/Cybersecurity Plans and Programs, Risk Management Oversight, and Federal Information Systems Management Act	Within 30 days of Task Order Award and updated monthly thereafter.	BPA Manager, COR, & each Government Section Lead.

(FISMA).		
Written Monthly Progress Report (MPR)	Emailed monthly; not later than the tenth working day of the following month.	COR, Government Project Lead
Written Monthly Financial Report	Emailed monthly; not later than the tenth working day of the following month.	BPA Manager, COR, Government Project Lead
Technical/Administrative Reports/Papers on DCIO Cybersecurity Capabilities/Areas of Interest	Within 10 days of Government tasking.	BPA Manager, Government Project Lead
Briefings/Presentations	Within 5 days of Government tasking.	Government Project Lead
Cost/Resource Assessment Summary on DCIO Cybersecurity Capabilities/Areas of Interest	Within 10 days of Government tasking.	Government Project Lead
Draft versions of white papers, policy documents and agreements	Within 60 days of tasking	Government Project Lead
Final versions of white papers, policy documents and agreements	Within 30 days of receipt of Government's comments on the draft	Government Project Lead
Draft versions of assessments, analyses, appraisals and strategy documents	Within 60 days of tasking	Government Project Lead
Final versions of assessments, analyses, appraisals and strategy documents	Within 30 days of receipt of Government's comments on the draft	Government Project Lead
Metrics, site map and content updates	Within 60 days of tasking	Government Project Lead
Draft versions of studies, plans and reports	Within 60 days of tasking	Government Project Lead

Final versions of studies, plans and reports	Within 30 days of receipt of Government's comments on the draft	Government Project Lead
Meetings support, pre- and post-event materials to include minutes	48 hours prior to the meeting 10 days following meeting	Government Project Lead
Spreadsheets and databases	Within 60 days of tasking	Government Project Lead

3.1.1 Deliverable Formats. All studies, analyses, reports, software, documentation, briefings, slides, etc. shall be prepared and presented in appropriate Microsoft Office application software: e.g., Word, Excel, Project, PowerPoint, etc. The applications shall be compatible with the versions installed at DoD CIO at the time the TWS is issued.

3.2 CONTRACTOR PERFORMANCE

A. Quality Control (QC). The Contractor's quality control program is the means by which it assures itself that its work complies with the requirements of the BPA and this task order.

B. Quality Assurance. The Government shall evaluate the Contractor's performance under this task order in accordance with the BPA Performance Requirement Summary (PRS), and Quality Assurance Surveillance Plan (QASP).

C. Government Remedies. The Contracting Officer shall follow FAR 52.212-4, "Contract Terms and Conditions-Commercial Items" or 52.246-4, "Inspection of Services-Fixed Price" for Contractor's failure to perform satisfactory services or failure to correct non-conforming services.

3.3 PERIOD OF PERFORMANCE

The period of performance for this task order shall be for one (1) base period of 12 months and four, 12-month option periods.

Base Period:	12 Months After Award
Option Period I:	12 Months After Base Period
Option Period II:	12 Months After Option Period I
Option Period III:	12 Months After Option Period II
Option Period IV:	12 Months After Option Period III

All support contractor personnel shall be at the place of performance at the beginning of the initial performance period.

3.4 HOURS OF OPERATION/PLACE OF PERFORMANCE

The primary place of performance will be in Government SCIFs in the National Capital Region such as in the Pentagon, Mark Center, Crystal City, Rosslyn, Fort Belvoir, or at surrounding metropolitan Washington, D.C. locations. Additionally, the Contractor's facilities in the Washington, D.C. metro area may be utilized. The Government will furnish office space and office equipment for work performed at Government facilities. The normal DoD CIO duty hours are 0800 to 1700 hours Monday through Friday, except Federal holidays or when the Government facility is closed due to local or national emergencies, administrative closings, or similar Government

directed facility closings. The Contractor must at all times maintain an adequate work force for the scope of work delineated within this task order when the Government facility is not closed for the above reasons.

Recognized Holidays: Unless required under the terms of the contract or authorized by the Contracting Officer, the Contractor shall not work on any of the following Government-observed legal holidays: New Year's Day; Birthday of Martin Luther King, Jr.; Presidents' Day (Observed); Memorial Day; Independence Day; Labor Day; Columbus Day; Veterans Day; Thanksgiving Day; and Christmas Day.

4.0 ESTIMATED LEVEL OF EFFORT

The Government estimates that this effort can be satisfied with approximately 33 FTE. The Government has the ability to accommodate up to 23 in DoD CIO offices. All personnel working under this task order must have a current Top Secret Clearance with SCI eligibility when the vendor proposal is submitted.

5.0 TRAVEL & ODCs

5.1 Travel - Travel is required to various CONUS/OCONUS locations as determined by the Government. In addition, some local travel may be required in conjunction with this task. Travel will not exceed **\$25,000.00** for the base period and **\$25,000.00** each option period. The Contractor shall provide a written request (e-mail) for travel to the COR prior to finalizing any travel arrangements. All travel must be approved by the COR prior to purchase of tickets and commencement of travel. The Contractor shall be reimbursed for actual allowable, allocable, and reasonable travel costs incurred during performance of this effort in accordance with the FAR 31.205-46 "Travel costs." and the Joint Travel Regulations, Volume 2, which applies to DoD civilian employees and others traveling at DoD expense. Requests for approval of costs in excess of maximum per diem rates in accordance with the procedures contained in FAR 31.205-46(a)(3) must be submitted to the Contracting Officer for final approval prior to commencement of travel.

5.2 ODCs – Conference Support - Contractor shall provide support for Government designated meetings and conferences in accordance with Paragraph 2.1.3 of the TWS, in the amount not-to-exceed **\$9,000** for the base period and **\$9,000.00** each option period. This cost reimbursable funding is intended for Government-specified engagement seminars, symposia, workshops, and forums explained in paragraph 2.1.3. These Government-approved events shall be submitted to and approved by either the Government technical POC from the supported DoD CIO Directorate, or the COR, prior to the event.

6.0 SECURITY

Personnel Security:

The DD254 (Contract Security Classification Specification) applies to this contract. All personnel working under this award must have a current Top Secret Clearance with SCI access.

Operations Security (OPSEC):

OPSEC is a structured process that identifies critical information, analyzes friendly actions, integrates threat analysis and risk assessments, then helps personnel apply protective measures to mitigate unacceptable risk.

The Contractor must comply with the same basic OPSEC rules, requirements, and standards as Government personnel. When Contractor personnel are working primarily in Government facilities, OPSEC Awareness Education and Training will be provided or coordinated through the appropriate Government security channels and OPSEC protective measures (countermeasures) will be applied as directed by the Government. All Contractor support personnel are required to receive OPSEC Awareness Education and Duty-Related Training.

The Contractor shall comply with the DoD Customers Operations Security Program, specifically DoDD 5205.02 "DoD Operations Security (OPSEC) Program," dated March 6, 2006.

7.0 GOVERNMENT FURNISHED PROPERTY OR EQUIPMENT

The Government shall provide the facilities, equipment, materials, and/or services listed below. Performance of this effort may require the Contractor to access and use data and information proprietary to a Government agency or Government Contractor which is of such a nature that its dissemination or use, other than in the performance of this effort, would be adverse to the interests of the Government and/or others.

As determined by mutual agreement, the Government will provide additional property that may be required in the performance of this effort.

At the request of the Government, or at completion of this effort, the Contractor will immediately return any Government-furnished property, including any equipment, specialized off-the-shelf software, and all other property provided by the Government for the Contractor to use to complete this effort.

- Information: The Government will provide the Contractors with access to relevant Government facilities, studies, reports, data, and key staff as required to perform the tasks contained in this TWS.
- Utilities: All utilities in the facility will be available for the Contractor's use in performance of duties outlined in this TWS. The Contractor shall instruct employees in utilities conservation practices. The Contractor shall be responsible for operating under conditions that preclude the waste of utilities.
- Facilities: The primary place of performance will be at Government facilities. When applicable, the Government will furnish the necessary workspace for the Contractor staff to provide the support outlined in this TWS to include desk space, telephones, computers, and other items necessary to maintain an office environment.

8.0 PROPRIETARY RIGHTS

All analyses, reports, documentation, briefings, etc., in whatever medium or format, developed and conducted under this task order are Government property. The Government will retain sole right to use, distribute, and/or publish these data and items as it sees fit.

9.0 TECHNICAL COGNIZANCE

The Contracting Officer's Representative (COR) for this effort will be designated in a separate delegation letter.

10.0 NON-DISCLOSURE AGREEMENT

In the course of performance pursuant to this contract, the Contractor will access nonpublic information, including Planning, Programming, Budgeting, and Execution (PPBE) information. The Contractor agrees that it will not use or disclose any such information unless authorized by the COR. The Contractor further agrees that it will use its best efforts to ensure that its employees and others performing services under this contract will not use or disclose any such information unless authorized by the COR. To that end, the Contractor agrees that each of its employees and others performing duties under this contract shall sign the Non-Disclosure Agreement set forth in Attachment 01-NDA.

11.0 MISCELLANEOUS ITEMS

11.1 POST AWARD CONFERENCE. The Contractor shall attend any post award conference convened by the Contracting Officer in accordance with Federal Acquisition Regulation Subpart 42.503.

11.2 WRITTEN REPORTING. To assist the Government with the appropriate surveillance during the performance of this TWS, a written Monthly Progress Report (MPR) is a requirement for this task order. MPRs will

be submitted via email to the Government Project Lead, COR., and BPA Manager. The primary objective of the report is to provide the Government reasonable assurance the contractor is using efficient methods and effective cost controls in executing each task. The contractor shall propose a format to be approved by the Government that meets the intent of the report, which shall include the following: 1) identification of fixed task order information, i.e. date of award of task order, period of performance of the task order, amount of award, anticipated completion date of the task order, 2) status of the order, 3) discussion of activities that map back to the tasks and deliverables identified in the task order including a summary of briefings, meetings, or visits and accomplishments during the reporting period; 4) milestones achieved; 5) anticipated activity for the next reporting period; 6) problems encountered or anticipated; 7) financial information including the amount of award by CLIN, invoiced costs for period submitted, amount invoiced to date, amount remaining, and % remaining, all submissions for travel costs shall include an explanation of the charges (contractor shall provide detailed back-up documentation for all travel costs as part of this MPR). Contractor will also provide detailed back-up documentation for all travel costs as part of its invoice submission; and 8) a forecast of the probability of completing the TWS within the required task order timeframe.

NDA

SUBJECT: NON DISCLOSURE AGREEMENT/OCI-PCI Representation

REFERENCE Contract No.:

CONTRACTOR:

I, _____, understand that, in the course of my employment with _____ (contractor), its subcontractors or consultants, I may, while providing services under the above contract, have access or routinely come into contact with non-public information and documents including, but not limited to, planning, programming, financial, budgeting or execution (PPBE) information, classified information, procurement information (e.g., future requirements, statements of work, and acquisition strategies), source selection information (e.g., bids, proposals, source selection plans, offeror evaluations and source selection decisions), trade secrets and other confidential/proprietary business information (e.g., confidential business information submitted by a contractor), attorney work product, attorney-client privilege information, Privacy Act-protected information (e.g., social security numbers, home addresses and telephone numbers) (PPI), or other sensitive data such as leases, internal memoranda and correspondence and a wide variety of other documents and information that must be safeguarded from disclosure (hereinafter "non-public information").

I agree that, as a condition to performing services under the above contract, I shall, in addition to any other obligations under federal law and regulations, not disclose, or cause to be disclosed, any non-public information without the prior written consent of the Contracting Officer or Contracting Officer's representative. I further agree that such non-public information will be safeguarded in accordance with Federal law and regulations and contractor's best commercial practices. I agree that I have an affirmative duty to determine whether a document/information are sensitive and not subject to public release before releasing or disclosing it to any Government agency, person or organization. I understand and agree that a failure to adequately safeguard such non-public information may result in termination of my employment, civil liability or criminal penalties.

I further understand that the duty to safeguard the non-public information is a continuing personal obligation that is not terminated or otherwise modified by change of jobs or employer. I further agree that upon ending employment with contractor, its subcontractor or consultant or termination of the above contract, I will return to contractor all non-public information in my possession.

I shall ensure that my status as a contractor employee is known when seeking access to and receiving non-public information from Government employees. Appropriate restrictive legends will be included on any copies or reproductions (paper or electronic) made of all non-public information and any data that is derived from, based upon, incorporates, includes or refers to the non-public information.

The duties described herein are in addition to, and independent of, any Procurement Integrity Certifications I may subsequently execute.

****These provisions are consistent with and do not supersede, conflict with, or otherwise alter the employee obligations, rights, or liabilities created by existing statute or Executive order relating to (1) classified information, (2) communications to Congress, (3) the reporting to an Inspector General of a violation of any law, rule, or regulation, or mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety, or (4) any other whistleblower protection. The definitions, requirements, obligations, rights, sanctions, and liabilities created by controlling Executive orders and statutory provisions are incorporated into this agreement and are controlling.****

I further represent that I have no past, present, or currently planned interest (financial or otherwise) relating to the work to be performed under this contract that would impinge my ability to render impartial, technically sound, and objective assistance or advice or in performing this contract. I further agree to disclose immediately to the Government any conflict of interest that arises after contract award to contractor. I also agree that I will not compete as an offeror or as a member of an offeror's team for any contract award that involves or relates to the services provided under the above referenced contract.

Signature: _____

Name: _____

Date: _____

OCI

SUBJECT: NON DISCLOSURE and OCI AGREEMENT/Representation

REFERENCE Contract No:

CONTRACTOR:

I, _____, as an authorized officer of contractor, acknowledge and agree on behalf of contractor, that, in the course of contractor's performance under the above contract, contractor may gain access or routinely come into contact with non-public information and documents including, but not limited to, planning, programming, financial,

budgeting or execution (PPBE) information, classified information, procurement information (e.g., future requirements, statements of work, and acquisition strategies), source selection information (e.g., bids, proposals, source selection plans, offeror evaluations and source selection decisions), trade secrets and other confidential/proprietary business information (e.g., confidential business information submitted by a contractor), attorney work product, attorney-client privilege information, Privacy Act-protected information (e.g., social security numbers, home addresses and telephone numbers) (PPI), or other sensitive data such as leases, internal memoranda and correspondence and a wide variety of other documents and information that must be safeguarded from disclosure (hereinafter "non-public information").

Contractor agrees that a condition to performing under the above contract, contractor, in addition to any other obligations under federal law and regulations, shall not disclose, or cause to be disclosed, any non-public information without the prior written consent of the Contracting Officer or Contracting Officer's representative. Contractor further agrees that such non-public information will be safeguarded in accordance with Federal law and regulations and contractor's best commercial practices. Contractor agrees that it has an affirmative duty to determine whether a document/ information are sensitive and not subject to public release before releasing or disclosing it to any Government entity, person or organization. Contractor understands and agrees that a failure to adequately safeguard non-public information may result in termination of the above contract and a variety of civil or criminal charges and penalties or both.

Contractor shall ensure that its status as a contractor is known when seeking access to and receiving non-public information from Government employees. Appropriate restrictive legends will be included by contractor on any copies or reproductions (paper or electronic) made of all non-public information and any data that is derived from, based upon, incorporates, includes or refers to the non-public information. Contractor will promptly (no later than one business day) report to the Contracting Officer or the Contracting Officer's representative any actual or suspected unauthorized use, disclosure, release, or reproduction of the non-public information or any violation of this agreement of which contractor is or may become aware

Contractor further understands and agrees that the duty to safeguard the non-public information is a continuing obligation that is not terminated or otherwise modified by contract expiration or termination. Contractor further agrees to bind all employees, subcontractors, suppliers, vendors and consultants to the non disclosure and conflict of interest obligations set forth in this agreement. Contractor further agrees that it will return all non-public information to the Federal Government or otherwise destroy the non-public information with the Government's written consent.

Contractor further represents that contractor has no past, present, or currently planned interest (financial, contractual, organizational, or otherwise) relating to the work to be performed under this contract that would impinge contractor's ability to render impartial, technically sound, and objective assistance or advice or result in it being given an unfair competitive advantage and that there exists no Organizational Conflict of Interest (OCI) as defined in FAR 9.5 that precludes contractor from performing this contract. Contractor further agrees to disclose immediately to the Government any OCI that arises after contract award to contractor. Contractor also agrees that it will not compete as an offeror or as a member of an offeror's team for any contract award that involves or relates to the services provided by contractor under the above referenced contract.

****These provisions are consistent with and do not supersede, conflict with, or otherwise alter the employee obligations, rights, or liabilities created by existing statute or Executive order relating to (1) classified information, (2) communications to Congress, (3) the reporting to an Inspector General of a violation of any law, rule, or regulation, or mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety, or (4) any other whistleblower protection. The definitions, requirements, obligations, rights, sanctions, and liabilities created by controlling Executive orders and statutory provisions are incorporated into this agreement and are controlling.****

The duties described herein are in addition to, and independent of, any Procurement Integrity Certifications contractor may subsequently execute.

Signature: _____

Name: _____

Date: _____

INSPECTION AND ACCEPTANCE TERMS

Supplies/services will be inspected/accepted at:

CLIN	INSPECT AT	INSPECT BY	ACCEPT AT	ACCEPT BY
0001	Destination	Government	Destination	Government
000101	Destination	Government	Destination	Government
000102	Destination	Government	Destination	Government
000103	Destination	Government	Destination	Government
000104	Destination	Government	Destination	Government
0002	Destination	Government	Destination	Government
0003	Destination	Government	Destination	Government
1001	Destination	Government	Destination	Government
1002	Destination	Government	Destination	Government
1003	Destination	Government	Destination	Government
2001	Destination	Government	Destination	Government
2002	Destination	Government	Destination	Government
2003	Destination	Government	Destination	Government
3001	Destination	Government	Destination	Government
3002	Destination	Government	Destination	Government
3003	Destination	Government	Destination	Government
4001	Destination	Government	Destination	Government
4002	Destination	Government	Destination	Government
4003	Destination	Government	Destination	Government

DELIVERY INFORMATION

CLIN	DELIVERY DATE	QUANTITY	SHIP TO ADDRESS	UIC
0001	POP 17-OCT-2014 TO 16-OCT-2015	N/A	OSD NII JOHN ROLANDO CRYSTAL MALL 3, SUITE 6032 ARLINGTON VA 22202 (b)(6) FOB: Destination	HQ0158
000101	N/A	N/A	N/A	N/A
000102	N/A	N/A	N/A	N/A
000103	N/A	N/A	N/A	N/A

000104	N/A	N/A	N/A	N/A
0002	POP 17-OCT-2014 TO 16-OCT-2015	N/A	OSD NII JOHN ROLANDO CRYSTAL MALL 3, SUITE 6032 ARLINGTON VA 22202 (b)(6) FOB: Destination	HQ0158
0003	POP 17-OCT-2014 TO 16-OCT-2015	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	HQ0158
1001	POP 17-OCT-2015 TO 16-OCT-2016	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	HQ0158
1002	POP 17-OCT-2015 TO 16-OCT-2016	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	HQ0158
1003	POP 17-OCT-2015 TO 16-OCT-2016	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	HQ0158
2001	POP 17-OCT-2016 TO 16-OCT-2017	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	HQ0158
2002	POP 17-OCT-2016 TO 16-OCT-2017	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	HQ0158
2003	POP 17-OCT-2016 TO 16-OCT-2017	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	HQ0158
3001	POP 17-OCT-2017 TO 16-OCT-2018	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	HQ0158
3002	POP 17-OCT-2017 TO 16-OCT-2018	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	HQ0158
3003	POP 17-OCT-2017 TO 16-OCT-2018	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	HQ0158
4001	POP 17-OCT-2018 TO 16-OCT-2019	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	HQ0158
4002	POP 17-OCT-2018 TO 16-OCT-2019	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	HQ0158
4003	POP 17-OCT-2018 TO 16-OCT-2019	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	HQ0158

ACCOUNTING AND APPROPRIATION DATA

AA: 97 5 0100.1120 00000 1522 251A 000000 049447 DSAC50279
 AMOUNT: (b)(4)
 CIN 00000000000000000000000000000000: (b)(4)

AB: 97 5 0100.1120 00000 1526 251A 000000 049447 DSAC50280
 AMOUNT: (b)(4)
 CIN 00000000000000000000000000000000: (b)(4)

AC: 97 5 0100.1120 00000 1527 251A 000000 049447 DSAC50281
 AMOUNT: (b)(4)
 CIN 00000000000000000000000000000000: (b)(4)

AD: 97 5 0100.1120 00000 1515 251A 96JU97 049447 DSAC50282
 AMOUNT: (b)(4)
 CIN 00000000000000000000000000000000: (b)(4)
 CIN HQ0158427302790001: \$25,000.00
 CIN HQ0158427302790002: \$9,000.00

CLAUSES INCORPORATED BY REFERENCE

52.204-9 Personal Identity Verification of Contractor Personnel JAN 2011

All clauses under contract GS-23F-9755H are hereby incorporated by reference.

CLAUSES INCORPORATED BY REFERENCE

52.204-10	Reporting Executive Compensation and First-Tier Subcontract Awards	JUL 2013
52.233-2	Service Of Protest	SEP 2006
252.201-7000	Contracting Officer's Representative	DEC 1991
252.204-7000	Disclosure Of Information	AUG 2013
252.227-7020	Rights In Special Works	JUN 1995
252.227-7021	Rights In Data--Existing Works	MAR 1979

CLAUSES INCORPORATED BY FULL TEXT

52.217-8 OPTION TO EXTEND SERVICES (NOV 1999)

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor within 30 days of contract expiration date.

(End of clause)

52.217-9 OPTION TO EXTEND THE TERM OF THE CONTRACT (MAR 2000)

(a) The Government may extend the term of this contract by written notice to the Contractor within 30 days of contract expiration date ; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 60 days before the contract expires. The preliminary notice does not commit the Government to an extension.

(b) If the Government exercises this option, the extended contract shall be considered to include this option clause.

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed 60 months.

(End of clause)

252.232-7006 WIDE AREA WORKFLOW PAYMENT INSTRUCTIONS (MAY 2013)

(a) Definitions. As used in this clause--

Department of Defense Activity Address Code (DoDAAC) is a six position code that uniquely identifies a unit, activity, or organization.

Document type means the type of payment request or receiving report available for creation in Wide Area WorkFlow (WAWF).

Local processing office (LPO) is the office responsible for payment certification when payment certification is done external to the entitlement system.

(b) Electronic invoicing. The WAWF system is the method to electronically process vendor payment requests and receiving reports, as authorized by DFARS 252.232-7003, Electronic Submission of Payment Requests and Receiving Reports.

(c) WAWF access. To access WAWF, the Contractor shall--

(1) Have a designated electronic business point of contact in the System for Award Management at <https://www.acquisition.gov>; and

(2) Be registered to use WAWF at <https://wawf.eb.mil/> following the step-by-step procedures for self-registration available at this Web site.

(d) WAWF training. The Contractor should follow the training instructions of the WAWF Web-Based Training Course and use the Practice Training Site before submitting payment requests through WAWF. Both can be accessed by selecting the "Web Based Training" link on the WAWF home page at <https://wawf.eb.mil/>.

(e) WAWF methods of document submission. Document submissions may be via Web entry, Electronic Data Interchange, or File Transfer Protocol.

(f) WAWF payment instructions. The Contractor must use the following information when submitting payment requests and receiving reports in WAWF for this contract/order:

(1) Document type. The Contractor shall use the following document type(s).

2 in 1 for Services only

(2) Inspection/acceptance location. The Contractor shall select the following inspection/acceptance location(s) in WAWF, as specified by the contracting officer.

HQ0158

(3) Document routing. The Contractor shall use the information in the Routing Data Table below only to fill in applicable fields in WAWF when creating payment requests and receiving reports in the system.

Routing Data Table*

Field Name in WAWF	Data to be entered in WAWF
Pay Official DoDAAC	HQ0347
Issue By DoDAAC	HQ0034
Admin DoDAAC	HQ0034
Inspect By DoDAAC	_____
Ship To Code	_____
Ship From Code	_____
Mark For Code	_____
Service Approver (DoDAAC)	_____
Service Acceptor (DoDAAC)	HQ0158
Accept at Other DoDAAC	_____
LPO DoDAAC	_____
DCAA Auditor DoDAAC	_____
Other DoDAAC(s)	_____

(4) Payment request and supporting documentation. The Contractor shall ensure a payment request includes appropriate contract line item and subline item descriptions of the work performed or supplies delivered, unit price/cost per unit, fee (if applicable), and all relevant back-up documentation, as defined in DFARS Appendix F, (e.g. timesheets) in support of each payment request.

(5) WAWF email notifications. The Contractor shall enter the email address identified below in the "Send Additional Email Notifications" field of WAWF once a document is submitted in the system.

DoD CIO, Mr. John Rolando: (b)(6)

(g) WAWF point of contact. (1) The Contractor may obtain clarification regarding invoicing in WAWF from the following contracting activity's WAWF point of contact.

NA

(2) For technical WAWF help, contact the WAWF helpdesk at 866-618-5988. (End of clause)

The contractor shall report ALL contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract via a secure data collection site. The contractor is required to completely fill in all required data fields using the following web address: <http://www.ecmra.mil/> <<http://www.ecmra.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, beginning with 2013. Contractors may direct technical questions to the help desk at: <http://www.ecmra.mil> <<http://www.ecmra.mil>> . [Reference: DPAP memorandum of 28 November 2012, "Enterprise-wide Contractor Manpower Reporting Application."]