ORDER FOR SUPPLIES OR SERVICES

PAGE OF PAGES: 1 | 15

IMPORTANT: Mark all packages and papers with contract and/or order numbers. BPA NO. BASIC

1. DATE OF ORDER: SEP 1 [redacted]	2. CONTRACT NO. (If any)
3. ORDER NO. / MODIFICATION NO.: DR-33-06-317-T070	4. REQUISITION/REFERENCE NO.: 33-06-317T070 DTD 8/4/2009

5. ISSUING OFFICE (Address correspondence to)
U.S. Nuclear Regulatory Commission
Div. of Contracts
Attn: Michele D. Sharpe
Mail Stop: TWB-01-B10M
Washington, DC 20555

6. SHIP TO:
a. NAME OF CONSIGNEE: U.S. Nuclear Regulatory Commission
b. STREET ADDRESS: Attn: Bill Dabbs, 11545 Rockville Pike, Mail Stop: T-2-C-2
c. CITY: Washington | d. STATE: DC | e. ZIP CODE: 20555

7. TO:
a. NAME OF CONTRACTOR: MAR, INCORPORATED
b. COMPANY NAME:
c. STREET ADDRESS: 1803 RESEARCH BLVD, SUITE 204
d. CITY: ROCKVILLE | e. STATE: MD | f. ZIP CODE: 208506106

f. SHIP VIA:

8. TYPE OF ORDER
[ ] a. PURCHASE — REFERENCE YOUR _____ Please furnish the following on the terms and conditions specified on both sides of this order and on the attached sheet, if any, including delivery as indicated.
[X] b. DELIVERY — Except for billing instructions on the reverse, this delivery order is subject to instructions contained on this side only of this form and is issued subject to the terms and conditions of the above-numbered contract.

9. ACCOUNTING AND APPROPRIATION DATA: $400,000.00
925-15-171-107 Q4171 252A 31X0200
FFS# 09631700171_0804c
DUNS# 062021639

10. REQUISITIONING OFFICE: CSO

11. BUSINESS CLASSIFICATION (Check appropriate box(es))
[X] a. SMALL [ ] b. OTHER THAN SMALL [ ] c. DISADVANTAGED [ ] g. SERVICE-DISABLED VETERAN-OWNED
[ ] d. WOMEN-OWNED [ ] e. HUBZone [ ] f. EMERGING SMALLBUSINESS

12. F.O.B. POINT: Destination

13. PLACE OF		14. GOVERNMENT B/L NO.	15. DELIVER TO F.O.B. POINT ON OR BEFORE (Date)	16. DISCOUNT TERMS
a. INSPECTION: Rockville, MD	b. ACCEPTANCE: Rockville, MD			

17. SCHEDULE (See reverse for Rejections) See CONTINUATION Page

ITEM NO. (a)	SUPPLIES OR SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
	TASK ORDER 70 UNDER NRC ORDER DR-33-06-317 (CISSS): The contractor shall provide the U.S. Nuclear Regulatory Commission (NRC) with, "Office of New Reactors (NRO) Continuous Monitoring Support" services in accordance with the following: -The attached Statement of Work (SOW) -The attached Schedule of Supplies and/or Services and Price -The terms and conditions of GSA Schedule GS-35F-0229K -The terms and conditions of NRC Order No. DR-33-06-317 Reference: MAR Quotation (Ref #2009-115/WA1529), dtd 9/11/09 ACCEPTED: Linda Klages 09/16/2009 Signature Date Linda Klages, VP, Contracts Print/Name and Title					

18. SHIPPING POINT	19. GROSS SHIPPING WEIGHT	20. INVOICE NO.		
			$445,554.70 (BASE YEAR)	17(h) TOTAL (Cont. pages)

SEE BILLING INSTRUCTIONS ON REVERSE

21. MAIL INVOICE TO:
a. NAME: Department of Interior / NBC, NRCPayments@nbc.gov
b. STREET ADDRESS (or P.O. Box): Attn: Fiscal Services Branch - D2770, 7301 W. Mansfield Avenue
c. CITY: Denver | d. STATE: CO | e. ZIP CODE: 80235-2230

$906,825.64 (BASE + OPT) — 17(i). GRAND TOTAL

22. UNITED STATES OF AMERICA BY (Signature): Eleni Jernell

23. NAME (Typed): Eleni Jernell
Contracting Officer
TITLE: CONTRACTING/ORDERING OFFICER

AUTHORIZED FOR LOCAL REPRODUCTION
PREVIOUS EDITION NOT USABLE

OPTIONAL FORM 347 (REV. 4/2006)
PRESCRIBED BY GSA/FAR 48 CFR 53.213(f)

TEMPLATE - ADM001 SUNSI REVIEW COMPLETE SEP 21 2009 ADM002

DELIVERY ORDER DR-33-06-317

TASK ORDER (70)

Office of New Reactors (NRO)

Continuous Monitoring

1.0 OBJECTIVE

The Contractor shall support the Office of New Reactors (NRO) Information System Security Program (ISSP).

2.0 BACKGROUND

For more information please review the system's security categorization document:

- EIG – Enterprise Information Gateway – This is a Major Application with an assumed sensitivity of: Confidentiality (**M**), Integrity (**M**), and Availability (**M**).
- EPM – Enterprise Project Management – This is a Major Application with an assumed sensitivity of Confidentiality (**M**), Integrity (**M**), and Availability (**M**).

3.0 PERIOD OF PERFORMANCE

This task order will have a period of performance for one year with one (1) one-year option:

	From	To	Condition
Base Year	Sept 18, 2009	Sept 17, 2010	N/A
Option Year 1	Sept 18, 2010	Sept 17, 2011	Only if Applicable Option Year of Base Contract is in Exercised

4.0 FUNDING

(a) The total estimated amount (ceiling) for the products/services ordered, delivered, and accepted under this task order is **$445,554.70** (includes **$5,000** for NTE travel).

(b) The amount presently obligated with respect to this task order is **$400,000**. The Contractor shall not be obligated to incur costs above this ceiling/obligated amount unless and until the Contracting Officer shall increase the amount obligated. When and if the amount(s) paid and payable to the Contractor hereunder shall equal the obligated amount, the Contractor shall not be obligated to continue performance of the work unless and until the Contracting Officer shall increase the amount obligated with respect to this contract. Any work undertaken by the Contractor in excess of the obligated amount specified is done so at the Contractor's sole risk.

5.0 SCOPE OF WORK

The Contractor must ensure NRO ISSP meets all federally mandated and Nuclear Regulatory Commission (NRC) defined security requirements. The Contractor shall perform the following: Integrated Security Activity Planning & Scheduling: Contingency Planning; Continuous Monitoring; and Other Technical Services

The Contractor shall provide the necessary security support staff to develop the associated documentation to support the tasks specified in Statement of Work (SOW) ENCLOSURE 6 of Delivery Order DR-33-06-317 "Certification and Accreditation (C&A) PROCESS AND DELIVERABLES".

6.0 TASKS

The Contractor shall support the NRO ISSP according to the Consolidated Information Security Support Services (CISSS) SOW Enclosure 6 and Section B "Schedule of Supplies or Services and Prices".

Please note that any Contractor personnel working under this task order can not take on the role of certification agent for any NRO system.

At no time is the Contractor allowed to configure an NRO operational system.

Subtask 1: Integrated Security Activity Project Plan

The Contractor shall develop and implement a project plan to ensure the completion of the tasks identified in this SOW occurs as expected. The Contractor shall be required to develop and maintain an Integrated Security Activity Project Plan and perform Integrated Activity Scheduling. These deliverables shall be developed at the individual project level (i.e., each system for which a certification and accreditation effort will be undertaken) and aggregate to the program level. The Project Plan shall incorporate all tasks and projects such that the individual projects roll up into an Integrated Security project schedule encompassing all NRC security related activities, services, and deliverables. The Project Plan shall identify resources for each activity and include the Work Breakdown Structure levels. The Project Plan will include:

- **Level 5 Work Breakdown Structure (WBS)**

  The WBS shall include a definition of the work to be conducted decomposed into distinct discrete manageable tasks or groups of tasks (work packages) with decisive outputs and specific measurable entry and exit criteria. Each work package shall have a short duration, or can be divided into a series of milestones whose status can be objectively measured. Each work package shall be assigned a start and finish date, a budget value, and can be integrated with higher-level schedules.

- **Schedule and Budget**

  The schedule and budget will identify what resources are needed, identify how much effort is required, and when each of the tasks specified in the WBS can be completed. The Contractor shall allocate a portion of the budget for each work package that comprises the WBS, and ensure that the WBS adequately defines all work necessary to meet the requirements for the project.

Subtask 2: Contingency Planning

The Contractor must ensure the each system's contingency planning process has been implemented according to federally mandated and Nuclear Regulatory Commission (NRC) defined security requirements. The Contractor will identify any deficiencies and will specify any operational risks that may affect the system's ability to perform its mission and protect its data (stored and transmitted). The Contractor shall perform the following:

Tasks	EIG	EPM
Subtask 2 – Contingency Plan (CP)	Update EIG contingency plan.	Update EPM contingency plan.

Tasks	EIG	EPM
Subtask 3 – Contingency Test and Report	The Contractor shall work with the system owner to verify, validate, and document the results of the system's contingency test. Upon completion of the Contingency Test, the Contractor shall update the system's Contingency Plan to reflect validated information.	The Contractor shall work with the system owner to verify, validate, and document the results of the system's contingency test. Upon completion of the Contingency Test, the Contractor shall update the system's Contingency Plan to reflect validated information.

The Contractor shall ensure that the steps, templates, and reports outlining the Contingency Planning process in NRC's Project Management Methodology are utilized and followed.

The Contractor shall provide the necessary security support staff to develop the associated documentation to support the tasks specified in Statement of Work (SOW) ENCLOSURE 6 of Delivery Order DR-33-06-317 "CERTIFICATION AND ACCREDITATION PROCESS AND DELIVERABLES" for unclassified systems.

2.1: System Contingency Planning

The Contractor shall support the NRC staff in the development and documentation of a Contingency Plan (CP) and test procedures. The System CP shall be documented in a report that follows the NRC Template for the System CP. The Plan shall be maintained in its hard copy form for contingency execution should the NRC Network Infrastructure be unavailable.

The CP shall be developed in accordance with federally mandated requirements, NRC defined security requirements, National Institute of Standards & Technology (NIST) Special Publication (SP) 800-34 "Contingency Planning Guide for Information Technology Systems", NIST SP 800-37 "Guide for the Security Certification & Accreditation of Federal Information Systems", and the NRC CP Template.

The Contractor shall provide detailed procedures for the Notification/Activation Phase, Recovery Operations, and Return to Normal Operations. The procedures shall contain sufficient detail that a technically trained individual not familiar with the system can successfully follow the procedures. The system CP shall contain

- Sufficient contact information (personnel and vendor)
- Equipment (hardware and software)
- Specification information to enable reconstitution of the system from scratch, all service level agreements, memoranda of understanding
- IT standard operating procedures for the system
- Identification of any systems that this system is dependent upon along with references for the applicable contingency plans
- References to the emergency management plan and occupant evacuation plan
- References to the appropriate continuity of operations plan.

The System CP shall be documented in a report that follows the NRC Template for System CP. The report shall be delivered in draft form and then in pre-Test form after NRC comments have been incorporated. The NRC CSO staff review of the draft is required to ensure compliance.

2.2: Contingency Test and Report

The Contractor shall provide expert advice and support during the Contingency Planning Test to ensure the test plan documentation is compliant with the System CP that has been approved by the NRC. Testing shall follow the test procedures developed and documented by the Contractor. The Contractor shall document the testing in a System Contingency Test Report (CP Test Report). The CP Test Report shall be developed in accordance with federally mandated requirements, NRC defined security requirements, NIST SP 800-34 "Contingency Planning Guide for Information Technology Systems", NIST SP 800-37 "Guide for the Security Certification and Accreditation of Federal Information Systems", and the NRC Contingency Test Report Template.

The CP Test shall be documented in a report that follows the NRC Template for NRC Contingency Test Report. The CP Test Report shall identify all testing assumptions, constraints, and dependencies as well as any anomalies, impromptu tests, and deviations encountered during testing. The CP Test Report shall include the actual testing schedule and detailed test results for each test procedure outlining specific errors encountered. The CP Test Report shall include a table of test findings incorporating any test issues and recommendations. The CP Test Report shall identify any problems encountered during testing and identify the resulting action items for the system. The CP Test Report shall be delivered in draft form and then in final form after NRC comments are incorporated. The NRC must approve the final CP Test Report.

The Contractor shall update the system's CP once the CP Test Report has been completed to reflect validated information. The NRC must approve the final version of the system's CP.

Subtask 3: Continuous Monitoring

This subtask contains the following elements:

3.1: Coordinate Continuous Monitoring Efforts

The Contractor shall assign a project manager to:

- Coordinate the efforts described in this task order.
- Serve as a point of contact between NRO & the Contractor.
- Manage the task's triple constraints, which are cost, time, and scope.
- Apply knowledge, skills, tools, and techniques to task order activities to meet or exceed NRO expectations.
- Work with NRO to ensure risks to their operational systems are minimized.
- Assist NRO in establishing their continuous monitoring schedules so federally mandated and NRC defined security requirements are met.
- Report at the weekly meeting all circumstances that impact the ability of the contractor to meet the stated objectives of this task order to the NRC Project Officer and NRO representative.
- Develop an agenda for the weekly status meeting and deliver that agenda to the NRC Project Officer and NRO representative by close of business each Monday.

3.2: Conduct Vulnerability Assessments

The Contractor shall conduct quarterly vulnerability assessments of NRO systems. These systems will include the following: EIG and EPM. More systems may be added at a later date via contract modification.

Vulnerability assessments shall establish if the system's security controls are operating as intended and ensure systems continually meet federally mandated and NRC defined security requirements. All risks / deficiencies shall be measured according to NIST SP 800-30 "Risk Management Guide for Information Technology Systems".

Tools

The contractor shall use a variety of testing tools (Nessus, Core Impact, DISA Gold, etc.), manual and automatic, including proprietary and modified open source, to conduct the assessment. Also, the contractor will need to employ specialized hardware and software to conduct wireless scans of E-SAFE and SGI-LAN. All hardware and software used to support this task order must be approved by the NRC Project Officer.

Process

This Vulnerability Assessment shall contain the following phases:

- Phase 1: Preparation – The contractor shall ensure all testing devices that are going to be used during the assessment are loaded with the latest patches, security updates, device drivers, and plug-ins.
- Phase 2: Information Gathering – The contractor shall conduct scans, review documentation, and interview personnel to gather the needed information to perform a risk analysis of NRO systems.
- Phase 3: Draft Assessment Reports - The contractor shall develop System Assessment Reports that identify the risks each system poses to itself, its data, and the NRC infrastructure.
- Phase 4: Validate Findings – The contractor shall work with the System Owner, ISSOs and System Administrators to validate the findings, ensure risks have been properly assessed, and to develop mitigation strategies that will resolve the deficiencies.
- Phase 5: Finalize Assessment Reports – The contractor shall incorporate NRC's comments into the Assessment Reports and deliverable the final version of the Assessment Reports to the NRC Project Officer.
- Phase 6: Summary Assessment Report – The contractor shall develop a Summary Assessment Report aggregating the findings across all NRO systems. The Summary Report shall document the overall risk the organization has incurred as well as any observed vulnerability trends.
- Phase 7: Plan of Action and Milestone (POA&M) Reports – The contractor shall incorporate any findings into each system's POA&M Report

The Assessment Reports, Summary Assessment Report, and Updated POA&M Reports shall be submitted to NRC Project Officer for review and comment. All reports must be approved by the NRC Project Officer, NRO System Owner, and NRO ISSOs. The Contractor shall revise and update each deliverable as appropriate and provide final versions to the NRC.

The contractor's Vulnerability Assessment Strategy shall include but will not be limited to the following:

- Identifying if the system is vulnerable to any published exploits
- Determining if the system has the latest patches installed
- Determining if the system is utilizing any unsupported hardware/software
- Analyzing if unnecessary ports or services are available
- Ensuring the system adheres to Federal regulations, guidelines, and standards
- Ensuring the system adheres to NRC hardening requirements
- Identifying if SANS top twenty or vendor identified vulnerabilities are present in the system
- Analyzing if the system's implementation adheres to the vendor's recommendations
- Ensuring the system's procedural controls are adequate
- Determining if the system's managerial controls are sufficient
- Analyzing weaknesses in the system's physical security
- Observing NRC employees, contractors, and vendors adherence to policy and procedures

Upon completion, the Contractor shall upload the test results and any resultant POA&M action items into the CSO FISMA tracking tool.

3.3: Annual Assessment

The Contractor shall conduct an annual assessment of NRO's information systems according to NIST SP 800-53A "Guide for Assessing the Security Controls in Federal Information Systems". The Contractor shall develop selection criteria to determine which security controls shall be tested. At a minimum, the selection criteria shall be based upon: the sensitivity level of the system; the requirement to annually test volatile controls; controls called out for annual testing in OMB guidance; CSO specified controls; and those associated with each system's POA&M items.

This assessment shall be performed on all NRO Major Applications and General Support Systems (EIG and EPM) during the 3rd quarter of each fiscal year.

The Contractor shall perform a comprehensive assessment of the selected management, operational, and technical security controls for each NRO system. The assessment shall determine the extent to which each system's controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting federally mandated and NRC defined security requirements. for each system consistent with NIST SP 800-53A.

Upon completion of testing the Contractor shall develop Annual Security Control Test Report for each system and incorporate any findings into each system's POA&M Report.

The draft Annual Security Control Test Reports and the POA& M Reports shall be submitted to NRO for review and comment. The Contractor shall revise and update each deliverable as appropriate and provide final versions to NRO.

Upon completion, the Contractor shall upload the Annual Assessment test results and any resultant POA&M action items into the CSO control tracking tool.

The annual assessment shall be done once a year.

3.4: Update NRO System Documentation

The Contractor shall update the C&A Package of all NRO Major Applications and General Support Systems (EIG and EPM).

The draft documents shall be submitted to NRO for review and comment. The Contractor shall revise and update each deliverable as appropriate and provide final versions to NRO.

This activity must be done in conjunction with the Annual Assessment. The update of NRO system documentation shall occur annually.

3.5: Reporting

Utilizing the NRC POA&M process, the Contractor shall update the POA&M Reports of all NRO Major Applications and General Support Systems quarterly.

The Contractor shall collect information so the POA&Ms can be updated to reflect the current situation. Any new vulnerability that is discovered shall be added and assigned to the appropriate system. All POA&M Reports shall be submitted to NRO for review and comment. The Contractor shall revise and update each deliverable as appropriate and provide final versions to NRO.

Upon completion, the Contractor shall upload the POA&M Reports into the CSO control tracking tool.

3.6: SGI Stand Alone Laptops and Desktops

NRO has standalone laptops and desktop systems: one that has removable media and one that does not.

For new SGI standalone laptops and desktops

- Update system documentation (memos and System Security Plans) to include the new component.
- Will scan any new SGI laptop or desktop to ensure security controls are operating as intended.
- Will deliver a report for each scanned SGI laptop or desktop that identifies its deficiencies.
- Will verify and validate that the patches for the SGI laptop or desktop are up to date.

For existing SGI standalone laptops and desktops, the contractor will:

- Update system documentation when the Laptops or Desktops are decommissioned.
- Ensure the memos and system security plans associated with these systems are updated annually to meet federally mandated and NRC defined security requirements.
- Will annually scan the laptops and desktops to ensure security controls are operating as intended.
- Work with NRO to design a method of patching their SGI laptops and desktops quarterly.

3.7: Unmanaged Unclassified non-SGI Laptops

NRO has unclassified non-SGI laptops that have been assigned to managers and staff for use at home or on travel.

For new laptops, the contractor will:

- Will scan any new laptop for Federal Desktop Core Configuration (FDCC) compliance.
- Will deliver a report for each scanned laptop that identifies its FDCC deficiencies.
- Will verify and validate that the patches for the new laptop are up to date.

For existing laptops, the contractor will:

- Will annually scan laptops to ensure FDCC compliance.
- Will deliver a report for each scanned laptop that identifies its FDCC deficiencies.
- Will deliver a summary report that extrapolates FDCC deficiencies across the organization.
- Work with NRO to design a method of patching these laptops quarterly.

Subtask 4: Other Technical Services.

This subtask contains the following elements:

4.1: Security Program Communications Support

The Contractor shall provide communications support when NRO is communicating with upper management, CSO staff, Office of Inspector General, or other responsible parties. Also, the Contractor will assist NISR NRO with their system specific and role based training.

4.2: Supporting Documentation

The Contractor shall develop documentation that identifies how the system's security controls have been implemented. Documentation will include details about the system's technical, managerial, and procedural controls.

Also, the Contractor will assist NRO in updating their rules of behavior (includes signing). Rules may exist for each system.

4.3: Security Engineering

The Contractor shall provide Security Engineering support to verify and validate the NRO proposed system architectures and implementations are based on sound security engineering principles and practices. The Contractor shall ensure that all federally mandated and NRC defined security requirements are met.

7.0 TRAVEL

Travel will not exceed $5,000 per year.

8.0 MEETINGS

The Contractor's Project Manager and technical lead shall attend weekly status meetings at NRC Headquarters every Wednesday with the NRC Project Officer and/or the NRO representative. This meeting will be used to discuss work being done under this task order and any issues that may have arisen during the last week.

TASK ORDER TERMS AND CONDITIONS

A.1 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 calendar days; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 60 calendar 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 two years.

A.2 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 task order. 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 1 year. The Contracting Officer may exercise the option by written notice to the Contractor within 60 days of the expiration of task order.

DELIVERY ORDER: DR-33-06-317
TASK ORDER: DR-33-06-317-T070
SCHEDULE OF PRICE AND/OR COST

Base Year - Option Year 3 Rates

Task Order Sub-Task Mapping	Schedule B Item Number	SOW REF	DELIVERABLE TITLE AND REQUIRED LABOR CATEGORIES FOR COMPLETION OF 1 DELIVERABLE FOR 1 SYSTEM	DISCOUNTED GSA LABOR RATE	HOURS FOR MAJOR SYSTEM	TOTAL AMOUNT FOR MAJOR SYSTEM	TO For reasons provided in Task Order Response	
					HIGH ONLY		Hours	Dollars
2.1	23	Encl 6	CONTINGENCY PLAN (1 SYSTEM)					
			Project Manager	$				
			QA Manager	$				
			Security Specialist IV	$				
			Security Specialist II	$				
			Documentation Specialist	$				
			Technical Writer II	$				
			Technical Writer I	$				
			TOTALS FOR CONTINGENCY PLAN (1 SYSTEM)					$ 20,049.07
2.2	24	Encl 6	CONTINGENCY PLAN REPORT (1 SYSTEM)					
			Project Manager	$				
			QA Manager	$				
			Security Specialist IV	$				
			Security Specialist III	$				
			Security Specialist II	$				
			Documentation Specialist	$				
			Technical Writer II	$				
			Technical Writer I	$				
			TOTALS FOR CONTINGENCY PLAN REPORT (1 SYSTEM)					
						SUBTASK 2 TOTAL	$	35,436.89
3.1	2	8.0	ACTIVITY SCHEDULING (ANNUAL)					
			Program Manager	$				
			Project Manager	$				
			QA Manager	$				
			Security Specialist IV	$				
			Security Specialist II	$				
			Sr. Financial Analyst	$				
			Documentation Specialist	$				
			Technical Writer II	$				
			Technical Writer I	$				
			TOTALS FOR ACTIVITY SCHEDULING (ANNUAL)					40,152.68
3.2	5	8.0	SECURITY SCANNING/PEN TEST (4 QUARTERS)					
			Project Manager	$				
			QA Manager	$				
			Security Specialist IV	$				
			Security Specialist II	$				
			Security Specialist I	$				
			Documentation Specialist	$				
			Technical Writer II	$				
			Technical Writer I	$				
			Network Security Analyst	$				
			TOTALS FOR SECURITY SCANNING/PEN TEST (4 QUARTERS)					43,956.64
3.3	14	Encl 6	ANNUAL ANALYSIS					
			Project Manager	$				
			QA Manager	$				
			Security Specialist IV	$				
			Security Specialist II	$				
			Security Specialist I	$				
			Documentation Specialist	$				
			Technical Writer II	$				
			Technical Writer I	$				
			TOTALS FOR ANNUAL ANALYSIS					$ 37,565.32

3.4	4	8.0	CONTROL VALIDATION (ANNUAL)				
			Project Manager	$			
			QA Manager	$			
			Security Specialist IV	$			
			Security Specialist II	$			
			Documentation Specialist	$			
			Technical Writer II	$			
			Technical Writer I	$			
			TOTALS FOR CONTROL VALIDATION (ANNUAL)				49,723.80
3.5	25	Encl 6	CORRECTIVE ACTION PLAN (1 SYSTEM)				
			Project Manager	$			
			QA Manager	$			
			Security Specialist IV	$			
			Security Specialist III	$			
			Security Specialist II	$			
			Documentation Specialist	$			
			Technical Writer II	$			
			Technical Writer I	$			
			Sr. Information Engineer	$			-
			TOTALS FOR CORRECTIVE ACTION PLAN (1 SYSTEM)				36,974.44
3.6	4	8.0	CONTROL VALIDATION (ANNUAL)				
			Project Manager	$			
			QA Manager	$			
			Security Specialist IV	$			
			Security Specialist II	$			
			Documentation Specialist	$			
			Technical Writer II	$			
			Technical Writer I	$			
			TOTALS FOR CONTROL VALIDATION (ANNUAL)				
3.7	4	8.0	CONTROL VALIDATION (ANNUAL)				
			Project Manager	$			
			QA Manager	$			
			Security Specialist IV	$			
			Security Specialist II	$			
			Documentation Specialist	$			
			Technical Writer II	$			
			Technical Writer I	$			
			TOTALS FOR CONTROL VALIDATION (ANNUAL)				
						SUBTASK 3 TOTAL	**$ 291,822.33**

4.1	16	Encl 6	SECURITY COMMUNICATIONS SUPPORT (ANNUAL)				
			Project Manager	$			
			QA Manager	$			
			Security Specialist IV	$			
			Security Specialist II	$			
			Technical Expert I	$			
			Documentation Specialist	$			
			Technical Writer II	$			
			Technical Writer I	$			
			TOTALS FOR SECURITY COMMUNICATIONS SUPPORT (ANNUAL)				36,974.44
4.2	7	8.0	SECURITY CONTOL MAINTENANCE (ANNUAL)				
			Project Manager	$			2,130.44
			QA Manager	$			516.22
			Security Specialist IV	$			1,577.35
			Security Specialist II	$			29,293.55
			Technical Expert I	$			-
			Documentation Specialist	$			1,759.16
			Technical Writer II	$			1,298.30
			Technical Writer I	$			1,198.33
			TOTALS FOR SECURITY CONTOL MAINTENANCE (ANNUAL)				$ 37,773.35

4.3	8	8.0	SECURITY ENGINEERING (ANNUAL)					
			Project Manager	$			$	
			QA Manager	$			$	
			Security Specialist IV	$			$	
			Security Specialist II	$			$	
			Senior INFOSEC Engineer	$			$	
			Subject Matter Expert III	$			$	
			Documentation Specialist	$			$	
			Technical Writer II	$			$	
			Technical Writer I	$			$	
			TOTALS FOR SECURITY ENGINEERING (ANNUAL)			$	$	38,547.68
							SUBTASK 4 TOTAL	**$ 113,295.47**

BASE YEAR TOTAL	**$ 440,554.70**
TRAVEL	**$ 5,000.00**
BASE YEAR GRAND TOTAL	**$ 445,554.70**

Option Year - Option Year 4 Rates

		SOW REF	DELIVERABLE TITLE AND REQUIRED LABOR CATEGORIES FOR COMPLETION OF 1 DELIVERABLE FOR 1 SYSTEM	DISCOUNTED GSA LABOR RATE	HOURS FOR MAJOR SYSTEM	TOTAL AMOUNT FOR MAJOR SYSTEM	TO For reasons provided in Task Order Response	
					HIGH ONLY		Hours	Dollars
2.1	23	Encl 6	CONTINGENCY PLAN (1 SYSTEM)					
			Project Manager	$				
			QA Manager	$				
			Security Specialist IV	$				
			Security Specialist II	$		$		
			Documentation Specialist	$		$		
			Technical Writer II	$		$		
			Technical Writer I	$		$		
			TOTALS FOR CONTINGENCY PLAN (1 SYSTEM)			$		$ 20,819.39
2.2	24	Encl 6	CONTINGENCY PLAN REPORT (1 SYSTEM)					
			Project Manager	$				
			QA Manager	$				
			Security Specialist IV	$				
			Security Specialist II	$				
			Security Specialist I	$	18			
			Documentation Specialist	$				
			Technical Writer II	$				
			Technical Writer I	$				
			TOTALS FOR CONTINGENCY PLAN REPORT (1 SYSTEM)			$		
							SUBTASK 2 TOTAL	**$ 36,810.50**

3.1	2	8.0	ACTIVITY SCHEDULING (ANNUAL)					
			Program Manager	$			$	-
			Project Manager	$			$	
			QA Manager	$			$	-
			Security Specialist IV	$			$	-
			Security Specialist II	$			$	-
			Sr. Financial Analyst	$		$	$	-
			Documentation Specialist	$			$	-
			Technical Writer II	$			$	
			Technical Writer I	$			$	
			TOTALS FOR ACTIVITY SCHEDULING (ANNUAL)			$	$	41,622.00

3.2	5	8.0	SECURITY SCANNING/PEN TEST (4 QUARTERS)			
			Project Manager	$		
			QA Manager	$		
			Security Specialist IV	$		
			Security Specialist II	$		
			Security Specialist I	$		
			Documentation Specialist	$		
			Technical Writer II	$		
			Technical Writer I	$		
			Network Security Analyst	$		
			TOTALS FOR SECURITY SCANNING/PEN TEST (4 QUARTERS)		$	$ 45,587.74
3.3	14	Encl 6	ANNUAL ANALYSIS			
			Project Manager	$		
			QA Manager	$		
			Security Specialist IV	$		
			Security Specialist II	$		
			Security Specialist I	$		
			Documentation Specialist	$		
			Technical Writer II	$		
			Technical Writer I	$		
			TOTALS FOR ANNUAL ANALYSIS		$	$ 38,959.30
3.4	4	8.0	CONTROL VALIDATION (ANNUAL)			
			Project Manager	$		
			QA Manager	$		
			Security Specialist IV	$		
			Security Specialist II	$		
			Documentation Specialist	$		
			Technical Writer II	$		
			Technical Writer I	$		
			TOTALS FOR CONTROL VALIDATION (ANNUAL)		$	50,878.49
3.5	25	Encl 6	CORRECTIVE ACTION PLAN (1 SYSTEM)			
			Project Manager	$		
			QA Manager	$		
			Security Specialist IV	$		
			Security Specialist II	$		
			Documentation Specialist	$		
			Technical Writer II	$		
			Technical Writer I	$		
			Sr. Information Engineer	$		
			TOTALS FOR CORRECTIVE ACTION PLAN (1 SYSTEM)		$	$ 38,346.48
3.6	4	8.0	CONTROL VALIDATION (ANNUAL)			
			Project Manager	$		
			QA Manager	$		
			Security Specialist IV	$		
			Security Specialist II	$		
			Documentation Specialist	$		
			Technical Writer II	$		
			Technical Writer I	$		
			TOTALS FOR CONTROL VALIDATION (ANNUAL)			43,283.40
3.7	4	8.0	CONTROL VALIDATION (ANNUAL)			
			Project Manager	$		
			QA Manager	$		
			Security Specialist IV	$		
			Security Specialist II	$		
			Documentation Specialist	$		
			Technical Writer II	$		
			Technical Writer I	$		
			TOTALS FOR CONTROL VALIDATION (ANNUAL)		$	$ 43,283.40
					SUBTASK 3 TOTAL	**$ 301,960.81**

4.1	16	Encl 6	SECURITY COMMUNICATIONS SUPPORT (ANNUAL)			
			Project Manager	$		$
			QA Manager	$		$
			Security Specialist IV	$		$
			Security Specialist II	$		$
			Technical Expert I	$		$
			Documentation Specialist	$		$
			Technical Writer II	$		$
			Technical Writer I	$		$
			TOTALS FOR SECURITY COMMUNICATIONS SUPPORT (ANNUAL)		$	$ 38,346.48
4.2	7	8.0	SECURITY CONTOL MAINTENANCE (ANNUAL)			
			Project Manager	$		$
			QA Manager	$		$
			Security Specialist IV	$		$
			Security Specialist II	$		$
			Technical Expert I	$		$
			Documentation Specialist	$		$
			Technical Writer II	$		$
			Technical Writer I	$		$
			TOTALS FOR SECURITY CONTOL MAINTENANCE (ANNUAL)		$	$ 39,175.04
4.3	8	8.0	SECURITY ENGINEERING (ANNUAL)			
			Project Manager	$		$
			QA Manager	$		$
			Security Specialist IV	$		$
			Security Specialist II	$		$
			Senior INFOSEC Engineer	$		$
			Subject Matter Expert III	$		$
			Documentation Specialist	$		$
			Technical Writer II	$		$
			Technical Writer I	$		$
			TOTALS FOR SECURITY ENGINEERING (ANNUAL)		$	$

SUBTASK 4 TOTAL $ 117,499.62

OPTION YEAR TOTAL $ 456,270.94
TRAVEL $ 5,000.00
OPTION YEAR GRAND TOTAL $ 461,270.94