LINDA L. KLAGES
Vice President

June 27, 2012

Contracting Officer
The U. S. Nuclear Regulatory Commission
Division of Contracts
12300 Twinbrook Parkway
Rockville, Maryland 20852

Subject: Response to Request for Quote (RFQ) No. NRC-HQ-12-R-33-0067, Amendments 1 through 4 Submission Date: June 27, 2012 4 PM EDT

Reference: MAR GSA Alliant SB GWAC Contract GS-06F-0641Z

Enclosures: Volume I – Technical
Volume II – Business/Cost
Attachment D – Price Schedule
MAR GSA Alliant Small Business Contract with modifications and pricing

Dear Mr. Pulaski:

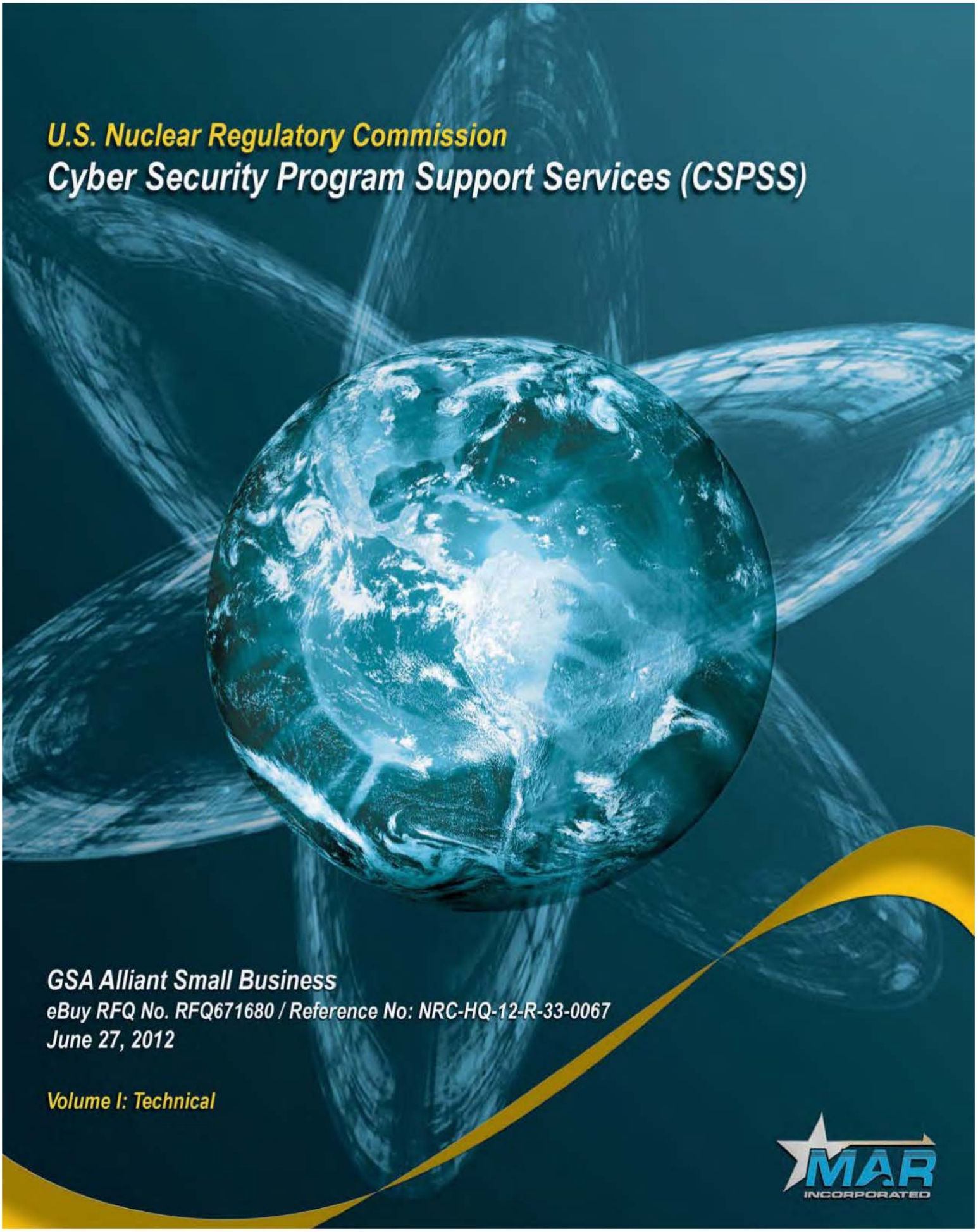
MAR, Incorporated is pleased to submit the enclosed proposal in response to the subject RFQ for Cyber Security Program Support Services (CSPSS). MAR certifies its status as a small business within the NAICS Code criteria set forth in our GSA Alliant SB Contract.

The proposal is valid until October 27, 2012. MAR takes no exception to the terms and conditions and provisions included in the solicitation. There are no current or former NRC employees involved either directly or indirectly in any part of this proposal.

We look forward to this opportunity and are available to respond to requests related to this quote. The following individuals are authorized to negotiate on behalf of the corporation: Ms. Linda L. Klages, Vice President, Contracts (301) 230-4576, lklages@marinc.com and Mr. Michael P. Norcio, Chairman and CEO (301) 230-4581 mnorcio@marinc.com

Sincerely,

Linda Klages
Vice President, Contracts



U.S. Nuclear Regulatory Commission
Cyber Security Program Support Services (CSPSS)

GSA Alliant Small Business
eBuy RFQ No. RFQ671680 / Reference No: NRC-HQ-12-R-33-0067
June 27, 2012

Volume I: Technical

MAR INCORPORATED

VOLUME I
TECHNICAL

RESPONSE TO:
RFQ NO.: 671680
REFERENCE NO.: NRC-HQ-12-R-33-0067
CYBER SECURITY PROGRAM SUPPORT SERVICES (CSPSS)

27 JUNE 2012

PREPARED FOR:
Nuclear Regulatory Commission
(NRC)

DELIVERED TO:
Jordan.pulaski@nrc.gov
Joseph.widdup@nrc.gov

ATTENTION:
Jordan Pulaski, Senior Contract Specialist
Joseph Widdup, Contracting Officer

SUBMITTED BY:
MAR, INCORPORATED
1803 Research Blvd, Suite 204, Rockville, MD 20850-6106

MAR PROPOSAL NUMBER: 2012-080/WA1685

This response includes data that is furnished in connection with RFQ No. 671680 and MAR Proposal Number 2012-080/WA1685 and shall not be disclosed outside the Government and shall not be duplicated, used, or disclosed – in whole or in part – for any purpose other than to evaluate this proposal. If, however, a contract is awarded to this offer or as a result of – or in connection with – the submission of this data, the Government shall have the right to duplicate, use, or disclose the data to the extent provided in the resulting contract. This restriction does not limit the Government's right to use information contained in this data if it is obtained from another source without restriction. The data subject to this restriction are contained in MAR Proposal Number 2012-080/WA1685.

Table of Contents

INTRODUCTION **1**
1.0 TECHNICAL APPROACH **4**
1.A Technical Understanding and Approach **4**
1.A.1 Project Management ***9***
1.A.1.1 Quality Assurance Plan (QAP) *9*
1.A.1.2 Project Plan (includes Level 4 Work Breakdown Structure) *14*
1.A.2 Special Projects ***17***
1.A.2.1 Assessment of Residual Risk *17*
1.A.2.2 Classified Processing Support *19*
1.A.2.3 Evaluation of New Technologies *19*
1.A.2.4 Analysis of Best Practices *20*
1.A.3 System Authorization ***21***
1.A.3.1 Obtaining NRC Information Systems Authorization to Operate *22*
1.A.3.2 Obtaining Laptop Authorization to Operate *33*
1.A.4 Continuous Monitoring Support ***34***
1.A.5 Data Calls ***40***
1.A.6 Cyber Situational Awareness ***41***
1.A.6.1 Incident Response Efforts *41*
1.A.6.2 NRC Enterprise Security Architecture *43*
1.A.6.3 Vulnerability Assessments *47*
1.A.6.4 Source Code Reviews *48*
1.A.6.5 Penetration Testing *49*
1.A.6.6 Security Impact Assessments *52*
1.A.7 Policy, Standards, and Training ***53***
1.A.7.1 Cyber Security Policy *53*
1.A.7.2 Processes, Procedures, Templates, Checklists, Standards, and Guidance *54*
1.A.7.3 Security Relevant Business Solutions *57*
1.A.7.4 Cyber Security Awareness Program *57*
1.A.7.5 Cyber Security Role-based Training Program *58*
1.A.7.6 Cyber Security Conference *61*
1.A.7.7 Electronically Communicating Cyber Security Information *64*
1.B MAR, Incorporated's Plan to Comply with FAR Clauses 52.219-6, 52.219-14, and 52.244-2 ..... **65**
2.0 Personnel Qualifications **66**
2.1 Resumes ..... **Resumes - 1**
2.1.1 Project Management Team ..... ***Resumes - 1***
2.1.1.1 Program Manager – George Simonds ..... *Resumes - 1*
2.1.1.2 Senior Project Manager – Thomas Evans ..... *Resumes - 5*
2.1.1.3 Project Manager – Michael Bernstein ..... *Resumes - 8*
2.1.1.4 Financial Analyst – Rebecca Quivey ..... *Resumes - 11*
2.1.1.5 Administration/Clerical (Senior) – Lauren Dickman ..... *Resumes - 13*
2.1.2 Quality Assurance Team ..... ***Resumes - 15***
2.1.2.1 Subject Matter Expert (Senior) – Hank Williams ..... *Resumes - 15*
2.1.2.2 Quality Assurance Specialist (Journeyman) – Sandra Smith ..... *Resumes - 20*

2.1.2.3 Quality Assurance Specialist (Journeyman) – Deborah Pollack....Resumes - 24
2.1.3 Technical Teams....Resumes - 26
2.1.3.1 Subject Matter Experts....Resumes - 26
2.1.3.2 Information Assurance/Security Specialists....Resumes - 38
2.1.3.3 Computer Forensic Intrusion Specialists....Resumes - 47
2.2 Staffing, Recruiting, and Retention....69
2.2.1 Staffing....69
2.2.2 Retention of Employees....69
2.2.3 Training....70
3.0 Corporate experience....70
3.1 Project Management (SOW Task 8.1)....71
3.2 Special Projects (SOW Task 8.2)....72
3.3 FISMA Compliance and Oversight (SOW Tasks 8.3, 8.4, 8.5)....72
3.4 Cyber Situational Awareness (SOW Task 8.6)....73
3.5 Policy, Standards, and Training (SOW Task 8.7)....74
4.0 Past Performance....75
4.1 List of Contracts (RFQ Attachment E)....75
4.2 Awards, Accolades, and Letters of Commendation....85
4.3 List of Terminated Contracts....88

List of Figures

Figure 1. NRC Cyber Security Program Evolution. 5
Figure 2. MAR Team CSPSS Integrated Project Approach and Understanding. 6
Figure 3. MAR CSPSS Project Organization and Functional Role. 7
Figure 4. MAR Program Management and Oversight System (PMOS). 8
Figure 5. MAR Quality Management Process. 10
Figure 6. Sample PMOS TaskTracker Module CSPSS Home Page. 15
Figure 7. NRC CISSS Project EVM History....16
Figure 8. MAR Team Residual Risk Assessment Process. 18
Figure 9. NIST Risk Management Framework....22
Figure 10. MAR Team System Authorization Process Aligned with NIST RMF. 23
Figure 11. Continuous Monitoring Process....35
Figure 12. Quarterly Scanning Process. 38
Figure 13. Data Call Response Lines of Communication 40
Figure 14. ESA activities follow the PMM and result in continuous maturity on an iterative basis. 44
Figure 15. Examples of Social Engineering Attacks. 51
Figure 16. Security Configuration Standard Lifecycle. 55
Figure 17. NRC and MAR Collaborative Course Development and Delivery Process. 59

List of Tables

Table 1. The MAR Team Strengths 2
Table 2. Organization of Technical Response in Accordance with RFQ 3
Table 3. Deficiency Prevention – Summary of Activities 11
Table 4. Work Breakdown Structure Levels and Descriptions 14
Table 5. NIST SP 800-53 18 Security Families 20
Table 6. ESA Deliverables 46
Table 7. NRC CSO Security Standard Lifecycle 55
Table 8. MAR Team GSA Alliant Small Business Labor Category Mapping to CSPSS Project Role 66
Table 9. Proposed Key Personnel Labor Categories, Education, and Certification 67
Table 10. Additional NRC Badged Resources 68

Description of Acronyms and Abbreviations

Acronym	Description
APT	Advanced Persistent Threat
ASB	Alliant Small Business
ASCT	Annual Security Control Testing
ATO	Authority to Operate
BIA	Business Impact Analysis
BPIAD	Business Process Improvement and Application Division
BPR	Business Process Reengineering
BYOD	Bring Your Own Device
C&A	Certification and Accreditation
CEO	Chief Executive Officer
CFIA	Computer Forensic and Intrusion Analyst
CFTC	Commodity Futures Trading Commission
CIS	Center for Internet Security
CISO	Chief Information Security Officer
CISSP	Certified Information Systems Security Professional
CISSS	Consolidated Information System Security Services
CLs	Cyber Labs
CLC	Corporate Lodging Corporation
CNSSI	Committee on National Security System Instruction
COBRA	Consolidated Omnibus Budget Reconciliation Act
COL	Combined License
CONOPS	Concept of Operations
CONUS	Contiguous United States
COR	Contracting Officer's Representative
COTS	Commercial off-the-shelf
CP	Contingency Plan(s)
CPIC	Capital Planning and Investment Control

Acronym	Description
CSA	Cyber Situational Awareness
CSAART	Cyber Situational Awareness Analysis Response Team
CSL	Cyber Solutions Lab
CSO	Computer Security Office
CSP	Cyber Security Program
CSPSS	Cyber Security Program Support Services
DAA	Designated Approving Authority
DFS	Division of Facilities and Security
DHCP	Dynamic Host Configuration Protocol
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DISA	Defense Information Systems Agency
DITSCAP	DoD Information Technology Security Certification and Accreditation Process
DNI	Director of National Intelligence
DOC	Department of Commerce
DoD	Department of Defense
DOE	Department of Energy
DOI	Department of Interior
DoJ	Department of Justice
DOL	Department of Labor
ECHO	Enforcement and Compliance History Online
EIGRP	Enhanced Interior Gateway Routing Protocol
EIT	electronic and information technology
EOUSA	Executive Office for United States Attorneys
EPA	Environmental Protection Agency
ERA	Enterprise Risk Assessment
ESA	Enterprise Security Architecture
EVM	Earned Value Management
FAR	Federal Acquisition Regulation
FBI	Federal Bureau of Investigation
FCOT	FISMA Compliance and Oversight Team
FEA	Federal Enterprise Architecture
FEMA	Federal Emergency Management Agency
FEMP	Federal Energy Management Program
FFP	Firm–Fixed-Price
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FRAP	Facilitated Risk Assessment Process
FSO	Facility Security Officer
FTS	Findings Tracking Sheet
FY	Fiscal Year
GAO	Government Accountability Office
GCIH	GIAC Certified Incident Handler
GIAC	Global Information Assurance Certification
GOTS	Government off-the-shelf

Acronym	Description
GSA	General Services Administration
GSA ASB	General Services Administration Alliant Small Business
GWAC	Government-wide Acquisition Contract
GWAPT	GIAC Web Application Penetration Tester
HQ	Headquarters
HSPD-12	Homeland Security Presidential Directive 12
IA/SS	Information Assurance/Security Specialist
IATO	Interim Authority to Operate
IAW	Indications, Analysis and Warnings systems
ICD	Intelligence Community Directive
ICOD	Infrastructure and Computer Operations Division
ICSJWG	Industrial Control System Joint Working Group
ID	Identification
IDS	Intrusion Detection Systems
IEC	International Electro-technical Commission
IIS	Microsoft Internet Information Services
ILTAB	International Laboratory for Tropical Agricultural Biotechnology
IM	Information Management
INFOCONs	Information Conditions
INPO	Institute of Nuclear Power Operations
IPR	Intellectual Property Rights
IPS	Intrusion Prevention Systems
IR	Incident Response
IRS	Internal Revenue Service
ISO	International Organization for Standardization
ISSO	Information System Security Officer(s)
IT	Information Technology
ITSRM	Information Technology Security Risk Management
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LMS	Learning Management System
LOB	Line of Business
MAC	Media Access Control
MAR	MAR Incorporated
MBSA	Microsoft Baseline Security Analyzer
MCT	Microsoft Certified Trainers
MCSE	Microsoft Certified Systems Engineer
MD	Management Directive
N/A	Not Applicable
NAT	Network Address Translation
NFS	Network File System
NIH	National Institute of Health
NIST	National Institute of Standards and Technology
NPP	Nuclear Power Plant
NRC	Nuclear Regulatory Commission

Acronym	Description
NRO	Office of New Reactors
NSA	National Security Agency
NSIR	Nuclear Security and Incident Response
OCOI	Organizational Conflict of Interests
OCONUS	Outside of Contiguous United States
ODC	Other Direct Cost(s)
OHMSETT	National Oil Spill Response Research & Renewable Energy Test Facility
OIG	Office of Inspector General
OIS	Office of Information Services
OMB	Office of Management and Budget
OPM	Office of Personnel Management
OS	Operating System
OTS	Office of Thrift Supervision
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
PM	Project Manager
PMM	Project Management Methodology
PMOS	Program Management Oversight System
PMP	Project Management Professional
POA&M	Plan of Action and Milestones
POC	Point of Contact
PPIRS	Past Performance Information Retrieval System
PST	Polices, Standards and Training
QA	Quality Assurance
QAP	Quality Assurance Plan
QC	Quality Control
QMS	Quality Management System
QSR	Quarterly Scanning Report
RAS	Remote Access Systems
RFP	Request for Proposal
RFQ	Request for Quotation
RMF	Risk Management Framework
ROI	Return on investment
RUP	Rational Unified Process
SA&A	Security Assessment and Authorization
SAAS	Software-As-A-Service
SANs	Storage Area Networks
SB/DFS	Security Branch, Division of Facilities and Security
SCA	Service Contract Act
SCAP	Security Content Automation Protocol
SCORM	Sharable Content Object Reference Model
SDLC	System Development Life Cycle
SEC	Securities and Exchange Commission

Acronym	Description
SES	Senior Executive Service
SGI	Safeguards Information
SIA	Security Impact Assessment(s)
SME	Subject Matter Expert(s)
SO	System Owner(s)
SOC	Security Operations Center
SOHO	Small Office Home Office
SOP	Standard operating procedure
SOW	Statement of Work
SP	Special Publication
SRA	Security Risk Assessment
SSAA	System Security Authorization Agreements
SSP	System Security Plan
ST&E	Systems Test and Evaluation
STP	Spanning Tree Protocol
SUNSI	Sensitive Unclassified Non-Safeguards Information
SWG	Standards Working Group
T&M	Time-and-Materials
TCP	Transmission Control Protocol
TO	Task Order(s)
TRB	Technical Review Board
TRM	Technical Reference Model
TSA	Transportation Security Administration
TS/SCI	Top Secret -Sensitive Compartmented Information
TW	Technical Writer
USGCB	United States Government Configuration Baseline
VAR	Vulnerability Assessment Report
VLAN	virtual local area networks
VM	Virtual Machine
VPN	Virtual Private Networking
VRL	Vulnerabilities Recommendations Library
VTP	VLAN Trunking Protocol
WAN	Wireless Area Network
WAP	Wireless Application Protocol
WBS	Work Breakdown Structure
WEP	Wired Equivalent Privacy
WINS	Windows Internet Name Service
XML	Extensible Markup Language

INTRODUCTION

MAR, Incorporated (MAR) is pleased to provide this proposal in response to the U. S. Nuclear Regulatory Commission's (NRC) Request for Quotation (RFQ) ID RFQ671680 under the General Services Administration (GSA) Alliant Small Business (ASB) Government Wide Acquisition Contract (GWAC). MAR, as GSA ASB GWAC prime contractor and as a proven provider of comprehensive Cyber Security services for the NRC, is honored to have the opportunity to continue our support to the government/industry team supporting the NRC by providing the services requested under the Cyber Security Program Support Services (CSPSS) project.

Our technical approach is a disciplined and structured one that is aligned with the NRC Project Management Methodology (PMM). Through our proposed approach, we will be positioned to assist the NRC with maintaining and maturing a robust enterprise Cyber Security Program on an on-going basis as future technical, programmatic, and regulatory requirements evolve.

The MAR Team's overall approach for the continued development, implementation, and sustainment support of NRC Cyber Security Program requirements include the following key features:

- Meeting and exceeding the immediate needs for each of the tasks and the associated NRC stakeholders through successful and measurable performance;
- Obtaining near-term program objectives while continuing to identify and implement program improvements to enhance day-to-day performance value; and
- Maintaining a pro-active vision and methodology for the long-term development of Cyber Security Program support services that adapt to changing cyber threats, regulatory compliance requirements, and mission needs to ensure an efficient, holistic risk management program.

The MAR Team

The proposed MAR Team includes selected companies from the current NRC Consolidated Information System Security Services (CISSS) contract Team established previously by MAR that were instrumental with assisting the NRC in successfully modernizing its security program over the past six years. New firms have been added to the Team to provide the depth and breadth needed to continue and strengthen our support of the NRC Computer Security Office (CSO) and NRC Program Offices. As a Team we will leverage our in-depth knowledge of NRC's mission, culture, and environment to assist in protecting its infrastructure through strong Cyber Security practices.

Through our GSA ASB Contract Number GS-06F-0641Z, MAR will manage our Team under Prime Contractor/Subcontractor arrangements where MAR is the prime contractor and all of the proposed team members are subcontractors.

MAR has assembled a team that has the capability and depth to perform the all of tasks outlined in the Statement of Work (SOW). These tasks and related activities will be closely monitored and managed as part of our program management responsibilities using our well-established program management practices, tools, and systems specifically developed over the past six years to align with NRC's processes and business needs. Additional details regarding MAR's Project Management capabilities are provided in Section 1.A.1.

Table 1 provides a brief overview of our individual Team members along with the experience and qualifications they each bring to the program. Additional individual company/organization details and the rationale for our selection of them as Team members are presented in Section 3.0, Corporate Experience.

Table 1. The MAR Team Strengths	
MAR Team Member	**Rationale for Selection**
MAR INCORPORATED	• In-depth knowledge and understanding of the NRC technology infrastructure, priorities, and culture. • Processes and tools in place to support contracts, management (financial tracking and staffing), and technical oversight built around the NRC CISSS contract and will be readily transitioned to the CSPSS project. • Trained, certified, and badged NRC knowledgeable authorized technical staff to support the main objectives of the RFQ. • ISO 9001:2008 Quality Management System certified. • ITIL Certified staff, PMP certified Managers.
CACI EVER VIGILANT®	• Leverage Cyber Solutions Lab (CSL) to evaluate new technologies that may be used under Special Projects. • Large reach back staff with extensive cyber security qualifications and certifications to support surge and Special Projects. • Expertise in ESA Support provided to DISA and the White House.
CONVERGENT solutions, inc.	• Current experience providing system authorizations and continuous monitoring for the U. S. Air Force and U. S. Army. • Enterprise security support to the U. S. Army.
DCCA Data Computer Corporation of America	• Cyber security expertise in classified environments. • Current experience providing system authorizations for Intelligence Community clients.
KNOWLEDGE consulting group KCG	• Currently supporting the NRC CSO Independent Verification and Validation activities for four years. • Ability to support cloud computing authorizations through their FedRAMP 3PAO accreditation. • Leverage SMEs in the areas of FISMA compliance, penetration testing, policies and procedure development, CPIC and Business Case planning, security architecture, and communication activities. • Support surge with their 240+ professionally certified IT security engineers serving the Federal Government market with over 400 security certifications.
Mainstay Enterprises, Inc.	• Currently providing specialized support to NRC for the CSO's FISMA compliance program. Plan of Action and Milestone (POA&M) activities, and the Incident Response Team over the past three years. • Specialized services to include information assurance and physical security. • Customers include the Air Force, Army, Housing and Urban Development, and Health and Human Services.
Prometheus Global	• Currently providing high profile cyber security services to the NRC for four years that includes: o Risk briefings including Advanced Persistent Threats (APT). o Development and delivery of security role-based training. o ESA. o Assessment of residual risk.
SECURICON Information Security Solutions	• Utilizes best practices in penetration testing, vulnerability assessments, and compliance assessments. • Supports Incident Response program development. • Provides Security Policy Development and Review support. • Customers include the Intelligence Community, Department of Defense, Department of Homeland Security, and Department of Transportation.
UNIVERSITY OF MARYLAND	• Access to cyber security alliances with academia, industry, and government through MAR's partnership with the Maryland Cyber Security Center (MC2). • Expertise in supply chain risk management, wireless and network security, attacker behavioral analysis, and economics of cyber security. • Comprehensive solutions to cyber security education, research, and technology development.

Pursuant to RFQ Section E.1, SOW Section 8, and Attachment H, MAR and all of our CSPSS Team members certify that **we are free of any Organizational Conflict of Interests (OCOI)** within the NRC. Additional details regarding the MAR Team's OCOI compliance are provided in Volume II – Business/Cost Section 3.0, MAR TEAM Responses to Provisions E.1 and E.4.

Organization of Technical Response in Accordance with RFQ

Table 2 presents the top-level organization of MAR's Technical Proposal in accordance with the RFQ and associated SOW.

Table 2. Organization of Technical Response in Accordance with RFQ

RFQ Section	RFQ Pg #	RFQ Section Title	MAR Proposal Section Number and Title	MAR Proposal Page #
E.9.1 E.10.1	E-5 E-6	Technical Approach	1.0 Technical Approach	4
E.9.1.A E.10.1.A	E-5 E-6	Technical Understanding and Approach	1.A Technical Understanding and Approach	4
SOW 8.1	4-5	Project Management	1.A.1 Project Management	9
SOW 8.2	5-6	Special Projects	1.A.2 Special Projects	17
SOW 8.3	6-13	System Authorization	1.A.3 System Authorization	21
SOW 8.4	13-15	Continuous Monitoring Support	1.A.4 Continuous Monitoring Support	34
SOW 8.5	15	Data Calls	1.A.5 Data Calls	40
SOW 8.6	15-22	Cyber Situational Awareness	1.A.6 Cyber Situational Awareness	41
SOW 8.7	22-31	Policy, Standards, and Training	1.A.7 Policy, Standards, Training	53
E.9.1.B E.10.1.B	E-5 E-6	Plan to Satisfy the requirements of FAR clauses 52.219-6, 52.219-14, and 52.244-2	1.B MAR Incorporated's Plan to Satisfy the requirements of FAR clauses 52.219-6, 52.219-14, and 52.244-2	65
E.9.2 E.10.2	E-5 E-6	Personnel Qualifications	2.0 Personnel Qualifications	66
E.9.3 E.10.3	E-5 E-7	Corporate Experience	3.0 Corporate Experience	70
E.9.4 E.10.4	E-6 E-7	Past Performance Information	4.0 Past Performance Information	75

Our proposal is fully responsive to the CSPSS RFQ and associated Statement of Work (SOW) and we take no exceptions to the RFQ. We believe our proposal represents the most cost effective, lowest-risk, and technically superior response to all of the requirements of the RFQ and is of greatest value to the NRC. All the identified staff in Section 2.0, Tables 9 and 10, are immediately available and fully capable of supporting the requirements outlined in this proposal. Furthermore, we believe our combination of highly experienced personnel and team-based management approach will position MAR to effectively support all requirements as stipulated in the RFQ. In Section 1.0, Technical Approach, we summarize our technical understanding and approach for each of the Tasks and deliverables associated with the RFQ technical requirements. Sections 1.A.1 through 1.A.7 describe the MAR Team's unique technical capabilities and approach to fully meet or exceed all requirements of the SOW. Section 2.0, Personnel Qualifications, along with Section 3.0, Corporate Experience, provides a summary of the specialized skills, relevant expertise, and demonstrated Corporate Experience the MAR Team will use in support of the RFQ and SOW requirements. Finally, MAR has provided a copy of the submitted Past Performance Questionnaires in Section 4.0, Past Performance.

1.0 TECHNICAL APPROACH

RFP Section E, pages 5-6

1.A Technical Understanding and Approach

RFP Section E, pages 5-6, SOW 1.0, pages 1-2

To provide maximum benefit to the NRC, MAR will employ a fully integrated team approach that will sustain the current success of the NRC's Cyber Security and Federal Information Security Management Act (FISMA) Compliance program and will support the program's continued maturity.

HIGHLIGHTS

- *MAR created over a dozen technical and management tools to specifically support the needs of the NRC CISSS contract and will also be used to support the CSPSS projects.*
- *Access to SMEs and industry recognized Cyber Security Experts.*
- *Access to state-of-the-art Cyber Labs and external penetration testing capabilities through team members CACI and KCG.*
- *Strong bench of personnel to support both day-to-day and surge requirements.*
- *Efficient management techniques on current CISSS contract resulting in a positive EVM allowing for the reallocation of funds back into the program will be used on CSPSS.*

MAR fully appreciates that the NRC is an integral part of protecting America's critical infrastructure. As an independent agency directly tasked with regulation and oversight as a primary mission objective, NRC collects, manages, and integrates classified and sensitive information from a variety of internal and external information sources. We understand it is imperative that the systems and resources used to manage and process data in these activities provide a secure and reliable environment to support the NRC mission. MAR also understands NRC's need to comply with Federal Cyber Security guidelines and current governing regulations. We will work with the NRC to continue to grow its Federally recognized FISMA (Federal Information Security Management Act of 2002) Compliance program, as noted in the March 7, 2012 *Office of Management and Budget (OMB) Fiscal Year 2011 Report to Congress on the Implementation of The Federal Information Security Management Act of 2002, page 38.* The report stated "The NRC, National Science Foundation, and Social Security Administration had compliant programs in place for all 11 areas, although each did identify areas for improvement. The remaining agencies had at least one area that needed significant improvement."

Historical Overview of MAR's Support Services for NRC's Information System Security Program

MAR looks forward to supporting the mission and operational Cyber Security needs of the NRC with a tightly integrated Technical and Management approach. Over the past six years, MAR has adapted to evolving security standards and the unique mission requirements of the NRC. Through the advanced training of our staff, and the development of improved templates, automated tools, and processes, we have significantly reduced the cost of deliverables and provided a consistent level of service. The NRC Cyber Security Program has made steady progress since the initiation and implementation of the CISSS contract which resulted with **all** operational systems receiving and maintaining an Authorization to Operate (ATO). Following the establishment of the NRC CSO, the program has experienced its challenges but also a documented succession of accomplishments. These accomplishments are the result of the dedicated collaboration between the CSO and its divisions (FISMA Compliance and Oversight Team (FCOT), Cyber Situational Awareness Team (CSA), and the Policies, Standards and Training Team (PSTT)), the Program Offices, and the supporting contractors including our MAR Team. ATOs and Contingency Plans (CPs) were the initial step in stabilizing the NRC Cyber Security Program. Once all ATOs were achieved, attention then turned to maintaining them through the implementation of a Continuous Monitoring Program with a focus on addressing agency level security requirements such as the development of security policies and procedures, role-based security

training, and an Enterprise Risk Assessment (ERA). Figure 1 highlights the evolution of the NRC Information System Security Program since the award of the CISSS contract to MAR in FY 2006, along with a look ahead toward growing the maturity of the program with continued enhancements within a robust stable Risk Management Framework (RMF). The MAR Team in partnership with the NRC has worked to establish and implement effective tools, processes, and standards, along with the right mix of qualified personnel and technical/management disciplines, to support the NRC's ability to meet Cyber Security Program milestones and on-going performance expectations.

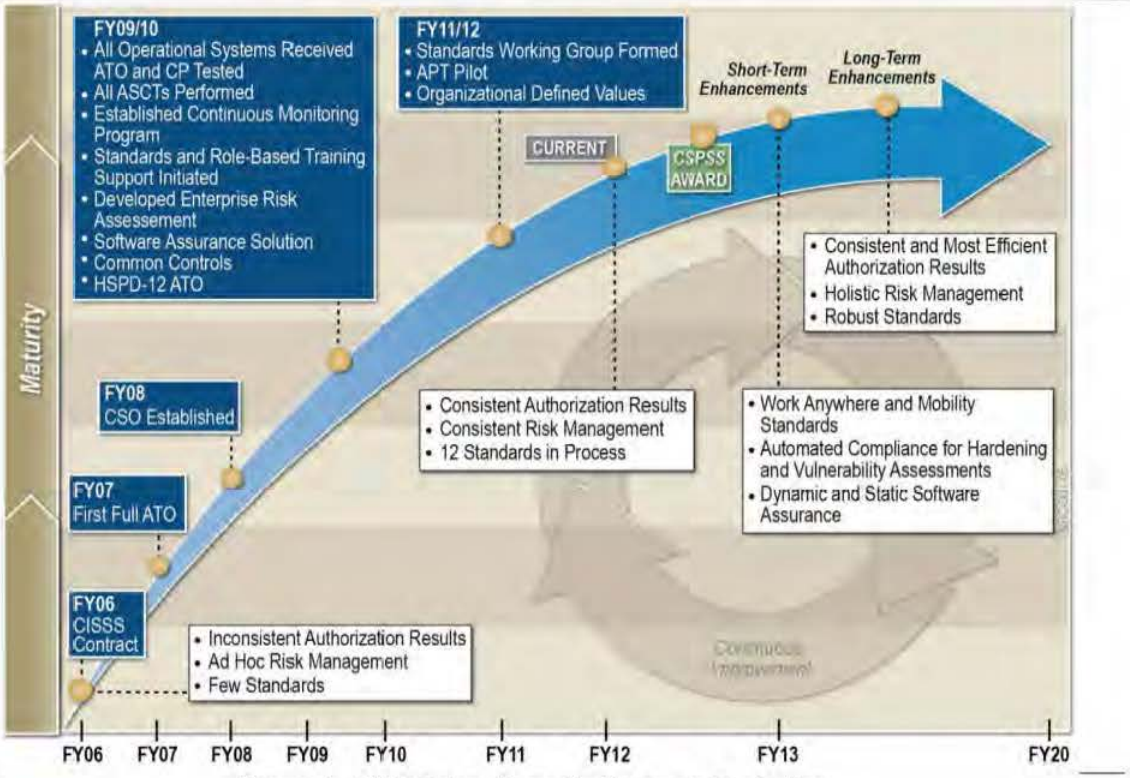


Figure 1. NRC Cyber Security Program Evolution.
The MAR Team will work with the NRC CSO and associated offices to continually mature the Cyber Security Program throughout the execution of the project.

Going forward, the MAR Team is prepared to assist and support the NRC by successfully performing the required tasks, providing the required deliverables, and introducing short- and long-term capability enhancements that will offer valuable program benefits to the NRC. Furthermore, these activities will assist in the development of a more robust Enterprise Security Architecture (ESA) that continuously matures the Cyber Security Program.

Summary of Proposed Technical Approach

The MAR Team technical approach, as shown in Figure 2, begins with our understanding of the NRC's Cyber Security and FISMA Compliance Program objectives and continues with the successful performance of the tasks and activities outlined in the SOW executed within the NRC's PMM framework. From the deliverables produced, detailed analytics are collected and reviewed on an ongoing basis with a focus towards enhancing governance and oversight in alignment with the NRC's mission. This approach will result in a more robust and mature Cyber Security Program for the NRC.

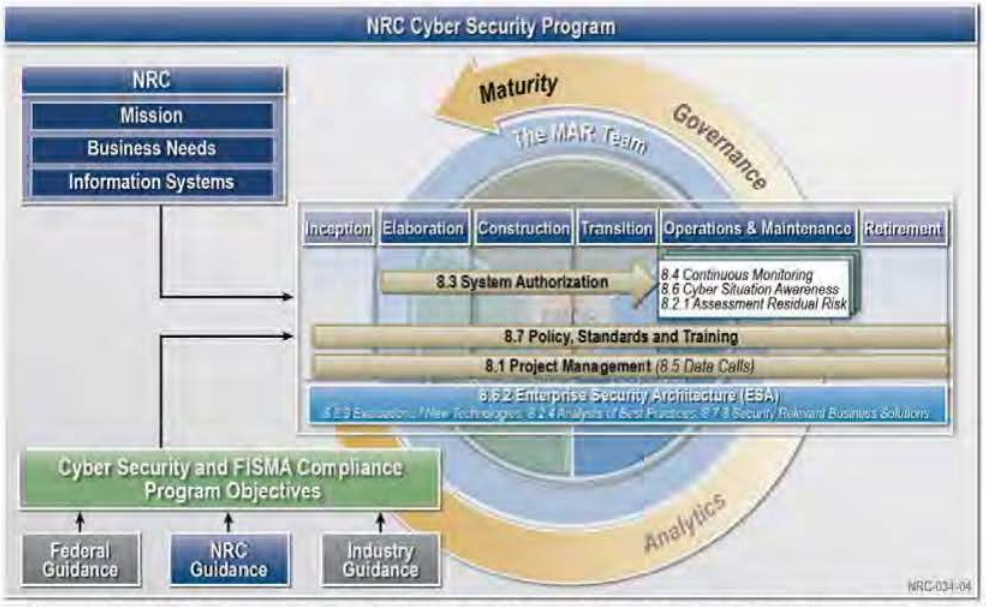


Figure 2. MAR Team CSPSS Integrated Project Approach and Understanding. The MAR Team's overall approach is to fully support all the objectives within the CSPSS Project while using our Team's experience in continuing to build a risk management framework across the NRC enterprise.

In each of the following sections, starting with Section 1.A.1, Project Management, we present our approach to delivering short and long-term improvements to the Cyber Security Program while working within the NRC PMM. We will work closely with all stakeholders to build upon NRC's FISMA accomplishments and assist the NRC in day-to-day FISMA activities, while also focusing on maturing ESA from a system level view of risk to managing risk at an enterprise-level in alignment with NIST SP 800-39. Section 1.A.6.2 presents the details of MAR's approach to support the NRC ESA.

At the core of our Team's support is MAR's proven Program Management and Oversight System (PMOS). Within PMOS is an integrated set of data repositories, portals, and support systems developed during the performance of the CISSS contract that we draw upon to assist in the analysis and production of security deliverables. Details of the PMOS are discussed on the following page.

CSPSS Project Organization

MAR's overall approach to managing the NRC CSPSS project addresses all components contained in the RFQ and SOW in support of the contract objectives. Figure 3 provides the proposed project organizational structure to support the NRC Cyber Security Program which consists of the Project Management, QA Oversight, and Technical Teams. The Technical Teams consist of an Integrated Project Team and Independent Assessment Team to align with the CSO teams and SOW Objectives. **The Independent Assessment Team is firewalled to ensure the integrity of all other activities that are conducted by the FISMA Compliance Team.** The QA Oversight Team, which is part of the Project Management Team, will oversee the technical content of deliverables and establish consistent criteria and processes for the Technical Teams. All program and financial activities will be managed by our experienced Project Management Team. Each team will have a Team Lead responsible for the overall coordination of activities. The Team Leads will work with the Project Managers to coordinate staffing resources to accomplish activities within the established timelines and budgets.

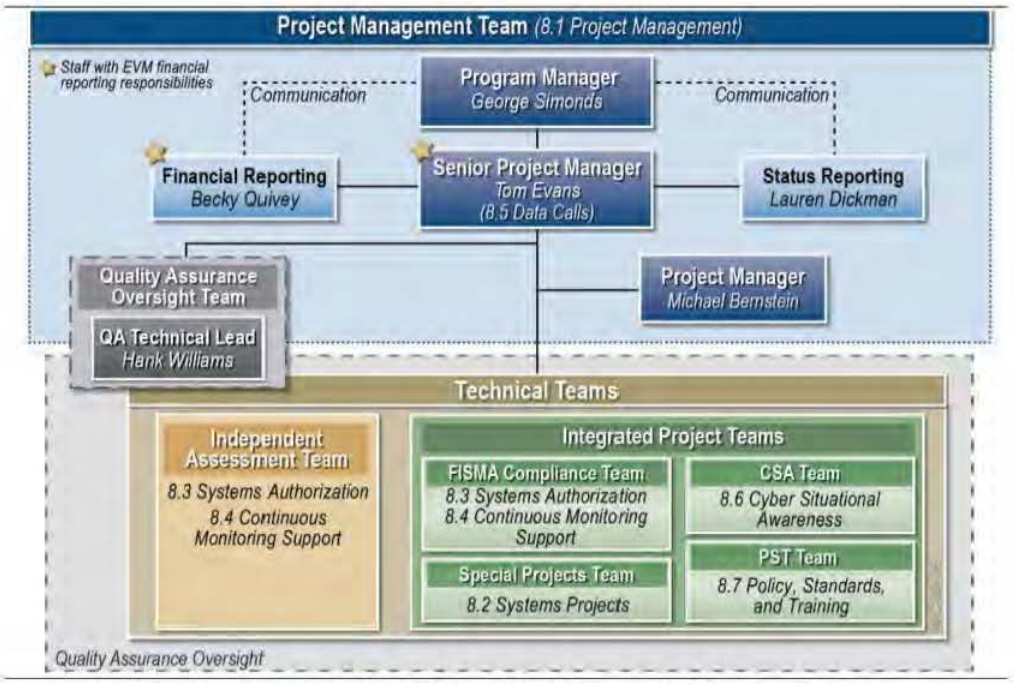


Figure 3. MAR CSPSS Project Organization and Functional Role. The MAR CSPSS Project Teams have been structured to align with the task and deliverable areas for the NRC CSPSS program.

Over the past six years MAR has maintained consistency in the key management and technical support personnel under the current CISSS program. We will continue to provide this same proven core team and have enhanced the organizational structure to add more technical expertise with improved quality oversight from the top down.

A critical component of the MAR Team organizational structure is the role of the Quality Assurance Oversight function which will ensure that technical content of deliverables is consistent with NRC criteria and processes. To support the delivery of quality services and deliverables on-time and on-budget, the MAR Team will continue the use of our Earned Value Management (EVM) system so that the NRC will have visibility into all technical and financial phases of the project. The MAR Team's EVM capabilities are supported by MAR's TaskTracker system, a component of the MAR PMOS, to integrate and measure cost, schedule, and technical accomplishments against established performance criteria and metrics.

MAR, Incorporated's Program Management and Oversight System (PMOS)

The management and delivery of services is based on a structured technical management approach with a standardized set of procedures and processes constructed for FISMA compliance and Cyber Security Program support activities. To support our ability to efficiently deliver these services, we use an integrated information management tool, tailored specifically for the NRC Cyber Security Program Support requirements. As depicted in Figure 4, this tool, the MAR PMOS provides Contractual, Technical, and Administrative/ Financial project information that is collected, processed, managed, accessed, and disseminated as a monitoring and reporting aid for the execution of our support services.

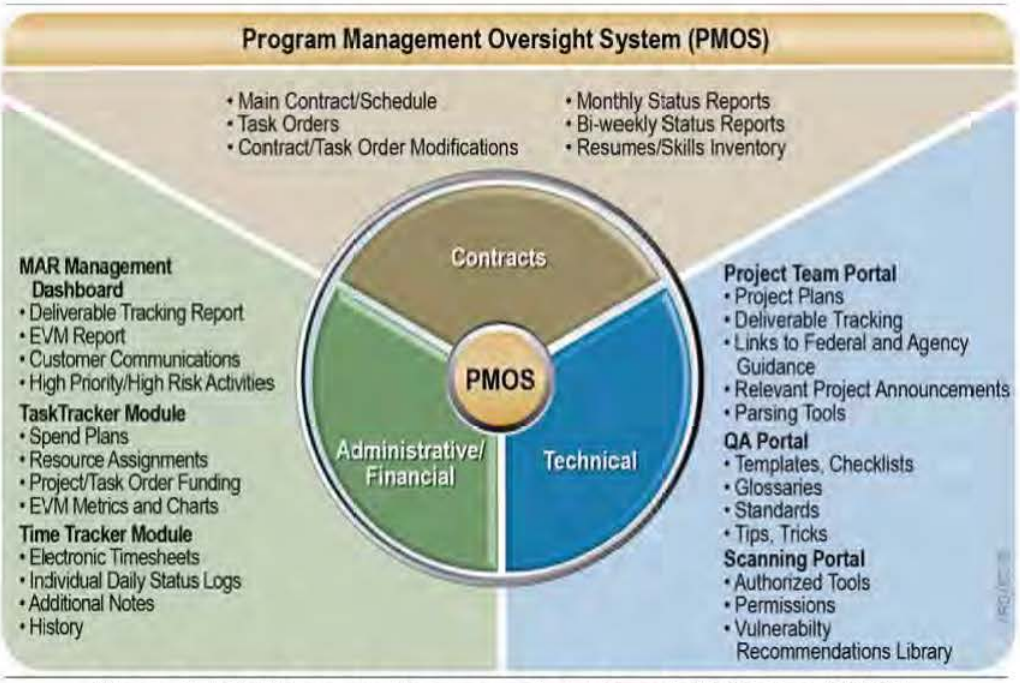


Figure 4. MAR Program Management and Oversight System (PMOS). PMOS is a MAR developed tool specifically tailored to manage the complex challenges of the NRC CISSS contract and will be made available for use on the CSPSS project.

Specifically, PMOS is a combination of data repositories and web-based tools that house performance metrics (contractual, administrative and financial, and technical), automated tools/scripts, templates, checklists, processes, tracking sheets, background information, and relevant data that are accessible to our Project Management, QA Oversight, and Technical Teams through a combination of web portals. PMOS includes:

- **Contracts Management –** The Contracts repository retains all program related documents including the main contract, task award, modifications, authorizations, and correspondence in a central location. The information is accessible through a portal to the CSPSS Project Management Team, MAR Executive Management, and the NRC.
- **Administrative/Financial Management –** The Administrative/Financial Mangement component is used to operate and monitor the day-to-day operations of the task. Two key systems within this component are MAR's custom developed TaskTracker and TimeTracker modules. TaskTracker maintains spend plans, resource assignments, and task funding which incorporates project plan completion data to prepare near real-time EVM charts and financial reports. TaskTracker is fully integrated with MAR's online timesheet entry system – TimeTracker. All MAR and subontractor staff on the task will be required to enter time into TimeTracker on a daily basis. Furthermore, TimeTracker requires a daily log of activities for all hours charged under the task.
- **Technical Management –** The Technical Management component is used by the Technical Teams as a key source for their day-to-day performance of work. There are three primary portals; Project Team, QA, and Scanning, each with associated data repositories, templates, checklists, links to internal and external references, and tools available to consistently produce security artifacts and deliverables.

We have incorporated the PMOS into every aspect of our current NRC CISSS contract and will seamlessly transition the PMOS to support the CSPSS project. The TaskTracker module has resulted in our Team's ability to provide daily monitoring and status reporting (financial and

technical) of program performance down to the activity/task level. All of these systems, along with their associated business practices, are well-established, fully implemented, and vital to delivering the quality professional support services NRC relies upon. We have aligned these systems and practices with NRC's Management Directive 2.8 and the NRC PMM. Additional details on the role of TaskTracker in support the CSPSS project are presented in Proposal Section 1.A.1.2.

1.A.1 Project Management

RFP Section E, pages 5-6, SOW 8.1, page 4

The institutional knowledge accumulated over the last six years, combined with our ability to continuously enhance and apply project management practices and tools, will support the progressive evolution of the NRC's Cyber Security Program.

HIGHLIGHTS

- *100% retention of MAR's Core NRC Program, Project, and Financial Management Team*
- *Established Technical and Management tools specifically for the NRC*
- *PMP certified Program/Project Managers*

To support adherenace to the NRC's Management Directive 2.8, MAR has developed an organizational structure that directly aligns with the NRC's Cyber Security Program main tasks and objectives, as shown in Figure 3. Our Project Management Team uses government recognized systems and processes for project oversight that includes: Deltek Accounting, Contracts/Subcontracts, Property Control, Security, Human Resources, Personnel Recruiting, and our integrated PMOS. Through the use of these systems and following ISO 9001:2008 standards, the MAR Team will ensure that the Cyber Security Program complies with all applicable Federal and NRC regulations, policies, standards, and guidance.

1.A.1.1 Quality Assurance Plan (QAP)

RFP Section E, pages 5-6, SOW 8.1.1, page 4

- *MAR's enhanced QAP is based on our ISO 9001:2008 Certified QMS.*
- *The MAR Team has implemented a TRB to provide an as-needed additional layer of QA oversight and guidance.*
- *The TRB is comprised of cyber security SMEs with broad range of experience, many with multiple years supporting the NRC.*

As a result of our six years of experience under CISSS, we have gained valuable lessons learned and have implemented best practices surrounding the development, review, delivery, and approval processes for all program artifacts. Our adoption of best practices and on-going incorporation of lessons learned have resulted in the documentation and implementation of improved processes that enable us to achieve repeatable, quality deliverables that are measurable and accountable against established metrics. This includes the establishment of the QA Portal within PMOS that stores checklists, templates, "Tips and Tricks" help guides, and schedules for sampling and inspections.

MAR also established a Technical Review Board (TRB) under the CISSS contract. The TRB is led by the proposed MAR Program Manager, George Simonds, and is comprised of NRC cleared Cyber Security Experts including Michael Shinn. Under the new CSPSS project, the TRB will be available to consult with Technical Teams and QA to offer expert guidance in circumstances where a second opinion may be needed. Tasks and their associated deliverables will continue to be completed to exceed NRC expectations, will be consistent, timely, and fully responsive to the specific technical requirements, and meet the established quality standards.

The foundation for the MAR Team's Quality Management System (QMS) is derived from the Quality Management Principles established by the ISO 9001:2008 standard. MAR's ISO 9001:2008 QMS involves a series of processes, procedures, and work instructions designed to ensure that all functions are properly executed and continually improved. The key elements of the MAR QMS are:

- Development of a formal quality assurance policy with specific procedures for each task area.

- Dissemination of the policy and procedures to all members of the MAR Team, accompanied by training to ensure that each member of our Team understands the policy and works toward a measurable objective.
- Execution of sound business decisions concerning the QMS based upon recorded data.
- Recording adequate accounts on all deliverables to allow problems to be traced to their source.
- Communication with the NRC about deliverables, inquiries, tasks, feedback and complaints.
- Regular assessment of performance through internal audits and reviews to drive improvements.
- Development of procedures for actual and potential nonconformance with established standards.

As shown in Figure 5, we will use the MAR ISO 9001:2008 QMS as a baseline to tailor specific quality control processes and procedures in preparing the proposed QA Plan (QAP) for the NRC CSPSS project. Our QAP is process-driven and designed to ensure a high quality, consistent level of performance across all task areas and deliverables.

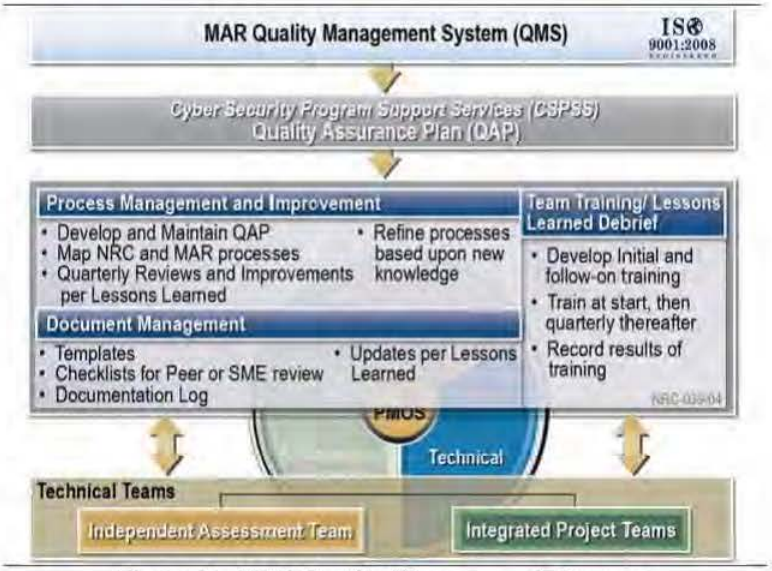


Figure 5. MAR Quality Management Process. The MAR QAP is based on MAR's ISO 9001:2008 Certified QMS and will be available to the MAR Team via the MAR PMOS.

The QAP focuses on three key functions within our deliverable management process 1) process management and improvement, 2) document management, and 3) team training and lessons learned debrief. This plan will be disseminated to the MAR Team during Team trainings and lessons learned debriefs, and will be stored in the QA Repository, component of the MAR PMOS, for CSPSS team members to access and review when preparing to perform their day-to-day activities. The QA Oversight Team will keep the QA modules up to date.

Pursuant to RFQ SOW Section 8.1.1, MAR developed the QAP using two major tenets of quality assurance; Deficiency Prevention and issue Resolution (corrective/preventative actions). To address Deficiency Prevention, MAR uses standardized processes tailored to each task area for creating, editing, reviewing, and approving all deliverables prior to their submission to the NRC. To address issue Resolution, MAR uses a process for responding in a timely manner to any deficiencies identified by either a MAR Team member or by the NRC. Additionally, the MAR Team uses a process improvement mechanism within the QAP to ensure that our deliverables continue to improve over time. Initial and quarterly training is provided to all MAR Team members to emphasize the importance of delivering quality products and task area results.

MAR is proposing Mr. Hank Williams as the QA Technical Lead for the NRC CSPSS project. Supporting Mr. Williams will be the TRB and a Technical Writer experienced in performing final reviews of cyber security artifacts for compliance with established styles and format. As the lead, Mr. Williams will be responsible for the performance and oversight of the following key functions within our deliverable management process:

- **Process Management and Improvement**
  - Update the QAP to a final, NRC approved plan and manage the implementation of the QAP throughout the life of the project.
  - Develop and document business processes for each task area.
  - Perform quarterly reviews with the NRC to gather feedback on the quality of the deliverables submitted.
  - Perform internal audits of the MAR processes and deliverables based upon standards set within the QAP.
  - Perform quarterly lessons learned reviews with key team members.
  - Refine MAR processes and procedures based upon this continuous feedback.
- **Document Management**
  - Control templates for each deliverable ensuring that the team uses the latest version.
  - Establish checklists for documentation peer or subject matter expert (SME) review.
  - Maintain documentation log and ensure all documents have completed the quality assurance process prior to submission.
  - Perform internal audits of the document management process.
  - Perform quarterly lessons learned reviews with key team members.
- **Team Training/Lessons Learned Debrief**
  - Develop initial/quarterly follow-on training on quality assurance procedures and processes.
  - Provide training for individual MAR Team members joining our Team and quarterly thereafter.
  - Maintain records of training on all MAR Team members.
  - Perform internal audits of the training materials and process.
  - Perform quarterly lessons learned reviews with key team members.

Deficiency Prevention

Table 3 presents MAR's CSPSS methodology for deficiency prevention which consists of three main activities: Standardization, Compliance Verification, and Adherence to Schedule and Budget.

Table 3. Deficiency Prevention – Summary of Activities

Standardization	Compliance Verification	Adherence to Schedule and Budget
• Use approved templates • Follow checklists for document preparation • Daily posting of drafts documents on NRC SharePoint or other approved secure repository	• Review SOW or related activity tasking • Review latest NIST or NRC Guidance • Review MAR QA Portal • PM/QA spot reviews of Daily Logs in TimeTracker • Unscheduled QA spot checks of deliverables	• Review Project Plan • Staffing and labor allocations posted in TaskTracker • Monitor financials in TaskTracker • EVM Reports • Bi-weekly Financial Reports • Status posted on Deliverable Tracker Dashboard

Standardization: The MAR Team will prepare all documents using approved NRC templates. QA will verify and instruct the Technical Team on the proper templates to be used for each activity. The templates can be either those currently in place at NRC or templates developed by the MAR Team and approved by the NRC/CSO for designated use. QA will also direct the Technical Team on the appropriate checklists and other MAR prepared reference materials that should be followed when preparing deliverable artifacts. An example of two such reference items:

- MAR/CISSS Deliverable Handbook which provides instructions for technical content associated with NRC FISMA compliance artifacts.
- NRC CISSS Contract Quality Assurance Checklist which provides a checklist of NRC and other related style guides to be followed when preparing NRC documents.

These and other related documents within MAR's PMOS will be updated when necessary to reflect CSPSS specific deliverable requirements.

Compliance Verification and Adherence to Schedule and Budget: MAR will use a series of both scheduled and unscheduled inspections to identify deficiencies and to verify that the Technical Teams supporting the NRC Cyber Security Program are using the approved templates; complying with applicable regulations, standards and procedures; and documenting systems information consistently across the enterprise. Technical Teams will be required to post daily all work in-progress on the designated NRC SharePoint site or other officially approved repository. The items will be available for QA spot inspections to verify compliance with appropriate templates, guidance, and validate that the status of the deliverables corresponds with the EVM metrics in TaskTracker. QA will immediately notify the Project Manager of any noted concerns or deficiencies.

Identifying Deficiencies - Scheduled Inspections

The MAR Team will use a document creation and review process as its methodology for performing scheduled inspections. This process consists of the following three steps:

1. **Document Creation:** The process begins with MAR's proposed Senior Project Manager (PM), Mr. Tom Evans, assigning responsibility for a specific task deliverable with a specified due date to a MAR Team member for completion. Depending on the complexity of the task and existing workloads, Mr. Evans may designate another Project Manager to assume responsibility for this task. The first draft of the deliverable will be created in the appropriate template after performing the research necessary to support the document. Once the document is completed and ready for review, a QA tracking sheet will be prepared for the document. The author will also notify the MAR Project Manager and the QA Technical Lead, Mr. Hank Williams, of any issues that arise which may affect the timely completion of a deliverable (unavailability of customer personnel or documentation, etc.). The MAR Project Manager will be responsible for reporting the issue to the NRC customer at the regularly scheduled status meetings, or earlier if necessary. Depending on the source of the delay, the Project Manager will either requests customer assistance in resolving the issue or request a modification of the initial due date for the deliverable.
2. **Document Review:** Upon initial completion of the draft document, Mr. Williams will assign a qualified staff member, usually a SME or a peer, to review the document. The staff member will review the document for any questionable or unusual research results, assumptions, or determinations. Document formatting and language will be reviewed for compliance with NRC/CSO structural and formatting standards. Any findings will be notated and discussed with the original author of the document to determine the necessary measures for remediation. In the event that an agreement cannot be reached, the issues will be elevated to Mr. Williams for resolution or to engage the TRB for assistance. Additional research or interviews may be conducted to ensure all modifications are accurately reflected in an updated draft of the document. Both the author and the reviewer will verify that version numbers are properly updated.
3. **Final Draft:** After all reviews and edits are completed, the author will mark the document as *FINAL DRAFT* and save it electronically in the document library. The author will update the library spreadsheet and forward the document with the accompanying QA tracking sheet to Mr. Williams.

Mr. Williams will perform a final review of the document and sign the accompanying QA tracking sheet and deliver the document. The document will be marked *DRAFT,* prepared for submission, and delivered to the designated NRC customer and the NRC Contracting Officer Representative (COR). The NRC COR will acknowledge receipt delivery. If the NRC accepts the draft without modification, the status will be updated to *FINAL* in the deliverable tracker. The acceptance notification will be filed within the document library.

If the NRC has comments or suggested edits to the final draft, the document will be returned to the author to respond to the NRC's feedback. The revised document will be re-submitted within the prescribed time period. The revised version will be reviewed by QA and delivered to the NRC. Upon

written acceptance by the NRC, the status will be altered to indicate a final deliverable and the appropriate metrics are updated by the PM.

Identifying Deficiencies - Unscheduled Inspections

Unscheduled inspections will be performed at random intervals by Mr. Williams or other MAR Team members as needed. Results of the inspections will be documented and maintained by Mr. Williams. Any deficiencies noted in the inspection are listed on the inspection check sheet along with the corresponding corrective action. The inspection is considered to be open as long as there are any open corrective actions. Once all corrective actions have been implemented, the inspection is considered closed. Lessons learned from the inspection are compiled and reported as part of the quarterly lessons learned meetings.

Resolution (Corrective/Preventative Actions)

The MAR Team will use our Corrective/Preventative Action process for problem resolution. As problems are identified they will be either resolved immediately or escalated. Regardless of the timeframe for resolution all problems are documented using a Corrective Action Form and Log that is maintained within the MAR PMOS.

The following information is provided in the Corrective Action Log: 1) a finding number and date, 2) source of the finding, 3) severity of the finding (i.e. major, minor, or observation), 4) a responsible party, 5) date of expected closure, and 6) description of the finding. Once the initial information has been logged, the Corrective Action Form is provided to the MAR Team member assigned to resolve the problem. The following information will be documented before closing the issue:

1. **Description:** The description includes a summary of the issue and how the MAR Team is made aware of it and if any policies or procedures were violated.
2. **Root Cause Analysis:** To completely resolve a problem all circumstances surrounding the issue must be understood. Root cause analysis is predicated on the belief that problems are best solved by attempting to correct or eliminate the root causes, as opposed to merely addressing the immediately obvious symptoms. By directing corrective measures at root causes the likelihood of problem recurrence will be minimized. To assist in doing this, the MAR Team uses the "5 Why" approach. By repeatedly asking the question "Why" the layers of symptoms which can lead to the root cause of a problem are removed.
3. **Corrective Action:** There may be instances when immediate/long-term actions are necessary. Those actions and the individual responsible for acting are identified here.
4. **Prevention Measures/Lessons Learned:** By finding the root cause preventative measures are developed and implemented within the organization. These may be captured during a lessons learned debrief that is conducted following each deliverable.
5. **Corrective Action Plan:** This plan identifies all actions that need to occur to correct the problem including revising documentation, disciplinary actions to be taken, or instituting peer reviews.
6. **Verification and Validation:** Once the corrective action plan is implemented a third party must review the implementation and document evidence of the corrective action and its effectiveness.

QA Wrap-up

Mr. Williams will conduct a lessons learned debrief upon completion of each task. Minutes of the debrief will be captured and compiled into a Lessons Learned Report and will include:

- Budget, Scope, or Timetable (Project Plan)
- Process, Policies, and Procedures
- Customer, Technical Team, or QA Concerns.
- Achievements – Customer and Team
- Recommendations

From lessons learned, our Team will review and update the templates or provide recommendations to the NRC CSO for improvements. We will work with the NRC and other contractors, when directed, to provide notification and dissemination to the Program Offices of any NRC approved changes to the processes, templates, and other related artifacts. QA will also work with CSPSS personnel to incorporate the recommended changes into other Task Areas including Cyber Security Awareness Program, Cyber Security Role-based Training, Cyber Security Conference, and Electronically communicating Cyber Security Information (CSO web site content and monthly newsletter).

1.A.1.2 Project Plan (includes Level 4 Work Breakdown Structure)

RFP Section E, pages 5-6, SOW 8.1.2, pages 4-5

Using the NRC's PMM Project Plan template, MAR will create a Project Plan within Microsoft Project to manage and oversee the CSPSS project. The Project Plan provides the framework for efficient execution of current CISSS projects, as well as future CSPSS projects and is the foundation of our Team's financial reporting capability. The Project Plan, integrated with the TaskTracker system, a component of the PMOS, provides daily tracking of individual task financial status and activities based on the Project Plan Work Breakdown Structures (WBS). Our Project Plans include a WBS through Level Five to effectively manage the activities related to the discreet task work packages. Descriptions for the Five WBS Levels are provided in Table 4.

- *Proven Management approach currently used under on existing CISSS resulting in an average of 30%-50% reduction in Task Order (TO) costs with a positive EVM expenditure level, as shown in Figure 7 on page 16.*
- *CISSS contract has not had monthly overages, nor has any task been over expended since October 2007*
- *Ability to remotely monitor daily status and activities through new technologies such as iPads, tablets, etc.*

Table 4. Work Breakdown Structure Levels and Descriptions

Level	Description
Level 1	Provides the name of the NRC Program Office that the activities are being performed for. MAR's TaskTracker module captures costs and EVM metrics at this level to support the requested reporting requirements.
Level 2	Provides the activity areas (8.3 System Authorization, 8.4 Continuous Monitoring Support, etc.) for each Program Office. MAR's TaskTracker module also captures costs and EVM metrics at this level to provide data for the NRC Bi-weekly Funding Report as well as other reports on an as requested basis.
Level 3	Provides the system name (if appropriate) and specific tasks that are being performed for each activity area. It is at this level that MAR establishes a schedule and ceiling for each distinct task along with the resources required to perform the work. MAR's TaskTracker module captures costs and EVM metrics at this level to provide reporting on an as requested basis to the Program Office and the CSPSS COR.
Level 4	Provides the discreet work packages necessary to complete the tasks outlined in Level 3. The work packages either have a short duration that will not exceed 80 hours or they will be divided into a series of milestones that can be used to objectively measure progress. All work packages have a start and finish date as well as a distinct budget value which roll up to create the overall Level 3 task ceiling.
Level 5	Provides the step-by-step processes necessary to complete the discreet work packages outlined in Level 4 (documentation collection, documentation creation, system scanning, QA review, etc.)

Project Plans are provided to Program Office CORs in PDF format and are also provided in .mmp file format for inclusion in the Monthly Status Report. All Program Office Project Plans are incorporated into an integrated master Project Plan for the CSPSS project that is also provided on a monthly basis to the NRC CSPSS COR in PDF format.

Throughout the lifecycle of the project, the Project Plan will be used as the primary means of capturing metrics related to timeliness and percentage of completion for EVM reporting purposes. As noted above, EVM reporting is accomplished using MAR's TaskTracker system, as shown in Figure 6. This system has been used for over five years on the current CISSS contract and has resulted in improved tracking of the overall financial and technical completion for each task.

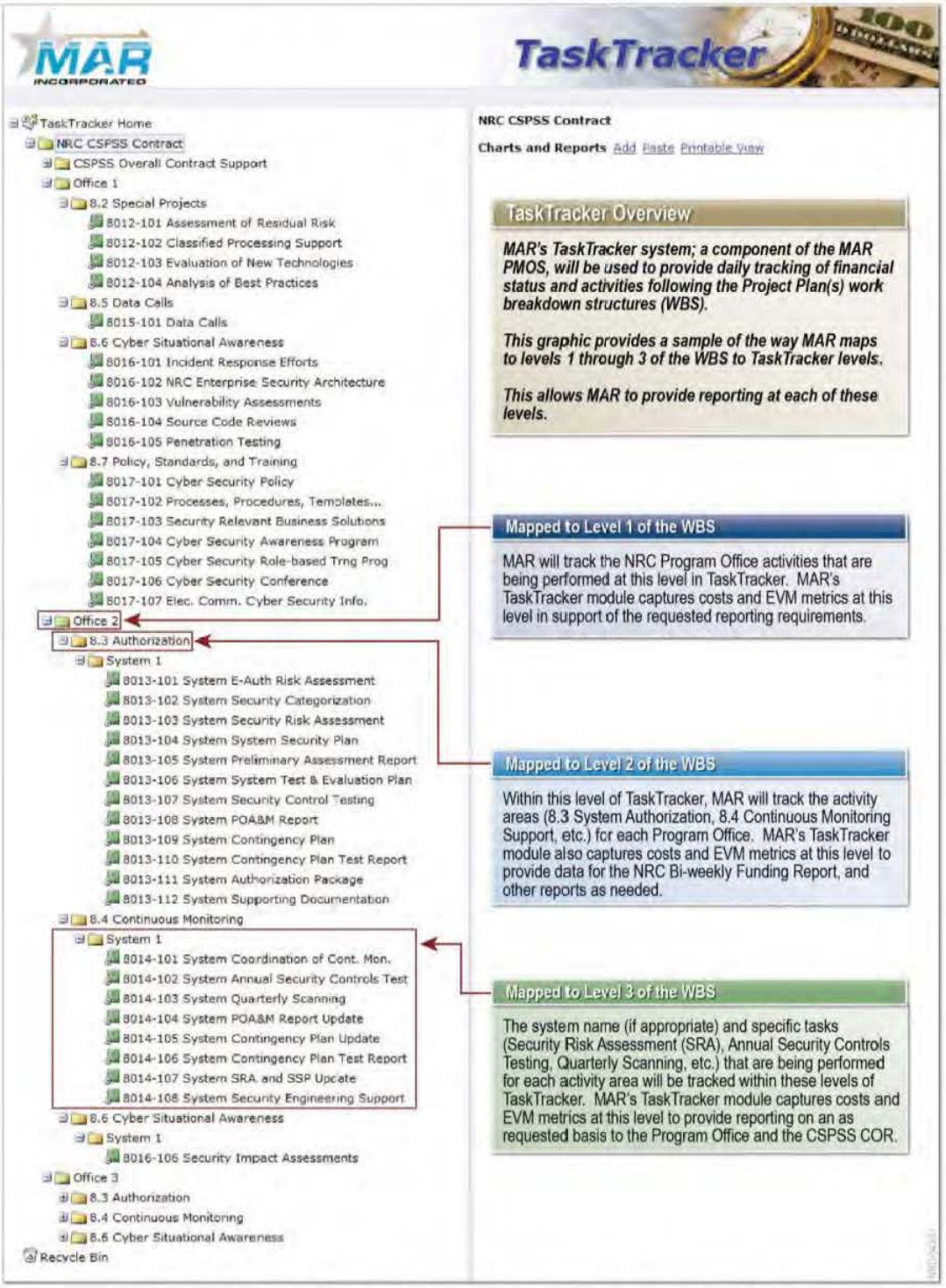


Figure 6. Sample PMOS TaskTracker Module CSPSS Home Page. By integrating the Project Plan WBS into the MAR TaskTracker system, the CSPSS Project Management Team will be able to provide EVM metrics at Levels One, Two, and Three of the WBS.

The Project Plans, together with TaskTracker, allow MAR to provide near real-time EVM metrics down to the Third Level, when needed. This approach, as currently used on the CISSS contract, has resulted in the MAR Team staying within prescribed schedules and budgets as shown in Figure 7. Upon implementation of TaskTracker, we were able to better track EVM metrics on a daily basis. Other important factors to highlight that coincide with program maturity, as previously shown in Figure 1, include the first full ATO, followed by the establishment of the CSO organization. The combination of these factors provided a level of standardization, which resulted in a positive cost variance for the duration of the CISSS contract.

Figure 7. NRC CISSS Project EVM History.
As the NRC Cyber Security Program matured, the MAR Team maintained a consistent positive EVM allowing reinvestment into the project.

MAR also uses a Dashboard function to manage and oversee tasks. The Management Dashboard is a component of the MAR PMOS and provides MAR Executive Management insight into contract/task performance through high-level program level metrics extracted from the Project Plan. Among these is the Deliverable Report list which provides a high-level view of the specific deliverable milestones from the Project Plan sorted by office, system, activity, and task in an automated two-week view. This view provides the current status of all deliverables throughout the document creation process.

The MAR Team understands the importance of using allocated funding in an efficient, appropriate, and consistent manner. As such, we periodically review, update, and revise Project Plans, spend plans, and financial and status reports to identify reductions in costs and timeframes where appropriate and practical. This approach is currently being used under our existing CISSS contract and has resulted in a significant reduction in specific TO costs.

Under expended funding was routinely reallocated back into the CISSS Task Orders providing added value to the NRC.

The TaskTracker system is also an integral part of supporting the Bi-weekly and Monthly financial and Status reporting requirements as it has the capability of capturing costs by activity down to the task level. The Bi-weekly report will be provided to the NRC CSPSS COR by the

close of business every other Tuesday and provides expenditures at the Second Level (Activity) of the WBS. The Bi-weekly reporting metrics (Office, Activity, Budget, Money Spent, Money Remaining, Remaining Labor, and Remaining ODC) are captured in MAR's TaskTracker system and used when providing the Bi-weekly report and on an as needed basis outside of the bi-weekly reporting cycle. The Monthly Progress report is provided to the CSPSS COR (together with monthly invoices), on MAR Corporate letterhead, no later than the close of business on the fifth calendar day of each month. This report contains the information specified in NRC's CSPSS RFQ Attachment 1, Monthly Progress Report Format.

MAR's PMOS TaskTracker component also provides near real-time reporting. MAR's timesheet system, TimeTracker, is integrated with TaskTracker and all timesheet (expenditure) and status entries are automatically available and updated upon entry. This function is used by the current CISSS COR on a daily basis.

1.A.2 Special Projects

RFP Section E, pages 5-6, SOW 8.2, page 5

The MAR Team has the staff expertise and corporate capabilities to assist the NRC in addressing Special Project initiatives. Senior analysts have been participants at industry conferences presenting on topics such as residual risk, implementing new technologies and applying best practices into existing and emerging programs.

HIGHLIGHTS

- *The MAR Team has conducted Executive Level APT Risk Briefing for the NRC.*
- *MAR and Prometheus authored the NRC Enterprise Risk Assessment (ERA) following NIST SP 800-39.*
- *MAR provides support to the Intelligence Community in development of risk mitigation strategies and classified system oversight.*
- *CACI will provide Cyber Lab capabilities to evaluate new technologies.*

The MAR Team understands the ever-evolving nature of Cyber Security and threats that are posed to the NRC and their mission. We will support special projects including the assessment of residual risk, classified processing support, evaluation of new technologies, and analysis of best practices. The resource availability and broad technical depth of our Team will provide the opportunity to bring personnel with proven multi-disciplinary expertise in these special project areas. We will be positioned to quickly respond to other challenges that may arise.

In the past, the MAR Team has collaborated with other federal agencies, including DOE, DHS, and EPA, to identify security best practices to provide the NRC with different perspectives on how other federal agencies are approaching Cyber Security program objectives. Additionally, the MAR Team has significant experience engaging vendors and evaluating vendor technologies to determine how they can support the objectives of the NRC Cyber Security program as well as those of other commercial and federal customers. In the following Sections we present our team's approach and the directly relevant experience we will bring to address NRC special projects requirements.

1.A.2.1 Assessment of Residual Risk

RFP Section E, pages 5-6, SOW 8.2.1, page 5

The MAR Team will conduct residual risk assessments to provide visibility into the remediation of known risks, to identify and determine impacts of previously unknown potential risks, and present mitigation strategies to address such risks. NIST 800-30 defines residual risk as the risk remaining after the implementation of controls for systems, programs, divisions, and for the agency-wide enterprise. The assessment focuses on residual risks to determine the acceptable and unacceptable levels of the risk by the NRC. These unacceptable levels of residual risk can be due to weaknesses in security controls related to programmatic, management, operational, and technical issues.

The residual risk assessments will be conducted on a quarterly basis and will focus specifically on risks impacting the enterprise level including multi-tier programs or multiple NRC information systems. Our Team has a working knowledge of many of the sources used to determine risks including:

- Audits – We will routinely review audit reports including GAO reports, OMB FISMA report to Congress, and the anticipated Continuous Authorization audits to determine risk impacts.
- Enterprise Risk Assessment (ERA) – MAR and team member Prometheus developed the current ERA. The ERA will be used as a guide in assessing risk impacts.
- Cyber Security Incidents – MAR team member Mainstay has supported the CSO's incident reporting and tracking. From this understanding we will review trends in formulating recommended actions.
- NRC Strategic Plans – We will routinely review the NRC Strategic Plan and its revisions as a guide in mapping risks to the NRC's mission.
- Inspector General Reports – Currently the MAR Team assists the NRC in responding to NRC OIG data calls and we recognize many of the risk focal areas. Our senior analysts will continue to review the annual NRC OIG FISMA report.
- Plan of Actions & Milestones (POA&M) – The MAR Team supports many of the NRC Program Offices in the preparation and updating of POA&Ms; we also support the CSO in the review and reporting of POA&M scorecards. These reports will be used as evidence of existing risks and the trends in remediation activities.
- Vendor Reported Vulnerabilities & Exploits – As part of our Quarterly Scanning and vulnerability assessment tasks we track potential vulnerabilities and exploits in our PMOS. This information will be used in the analysis and prioritizing of risks.
- Observations – We will draw upon our familiarity of NRC systems and understanding of business needs to assist in mapping risks to the NRC mission.

Our proposed process for developing the Residual Risk Assessment Quarterly Report and Briefing Process is outlined in Figure 8.

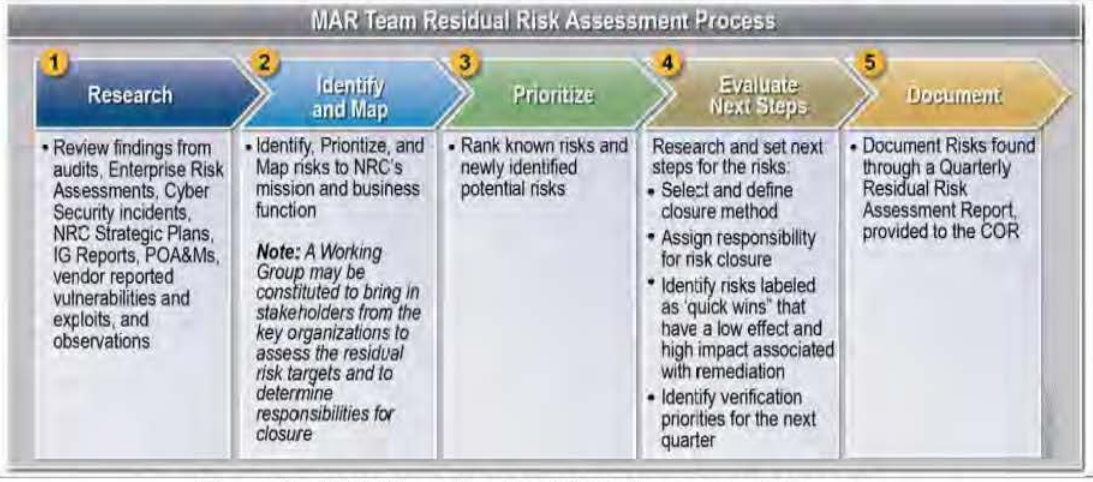


Figure 8. MAR Team Residual Risk Assessment Process.
The MAR Team will take a NIST 800-30 based systematic approach to Residual Risk Assessments.

Using our knowledge of the NRC infrastructure and source documents outlined in the SOW, we will conduct in-depth research to identify and map risks to the NRC's mission. From this mapping we will prioritize the risks and evaluate the next steps for the identified risks. The MAR Team will work with each of the CSO teams, our ESA Team, and the Policy, Standards, and Training Team to ensure standard risk ratings and priorities are defined and consistently applied across all

possible risk activities. The Senior Project Manager, Mr. Evans, will coordinate with the COR on the report format and schedule the quarterly briefing. MAR senior cyber security analysts will conduct the quarterly residual risk assessment briefing to the NRC CSO and management.

1.A.2.2 Classified Processing Support

RFP Section E, pages 5-6, SOW 8.2.2, pages 5-6

- *The MAR Team has NRC Q-cleared TS/ SCI personnel with additional reach back to more TS/ SCI personnel to support classified system support.*
- *Within the Intelligence Community, MAR oversees the authorizations for approximately 120 classified systems.*

The MAR Team currently has NRC Q-cleared TS SCI personnel on staff that will support security engineering support and also classified systems authorization and continuous monitoring activities. Our approach to ensuring NRC is authorized to operate systems that process classified information focuses on strengthening existing information security controls as well as implementing new controls. The MAR Team will continue to use the following documents when developing specific actions:

- **ICD-503** Intelligence Community Directive Number 503 – Information Technology Systems Security Risk Management, Certification and Accreditation.
- **NIST SP 800-37** Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle.
- **CNSSI-1253** Committee on National Security Systems Instruction No. 1253 – Security Categorization and Control Selection for National Security Systems.
- **NIST SP 800-53** Recommended Security Controls for Federal Information Systems and Organizations.

The MAR Team will draw upon our analysts with classified system support experience to analyze existing security controls and review the current control environment with key NRC personnel, including people, processes, and technologies. This will result in a document capturing the current security posture of the NRC organization to put in place a process for preparing classified system authorization to operate packages. This process will outline the actions required to bring each system into compliance with ICD-503. Each action will be directly linked to one or more security controls found in NIST SP 800-53. Using this process our analysts will support the NRC efforts in obtaining an authorization to operate for the systems processing classified information.

We will also establish a formal continuous monitoring program for information systems that process classified information at the NRC. This program will assist in bringing systems into compliance, and also protect the NRC investment in information security by maintaining compliance into the future as the risks and threats surrounding information technology evolve.

This approach provides all parties involved with a method to monitor the progress of the NRC systems that process classified information in alignment with the ongoing development of the NRC's agency wide information security program.

1.A.2.3 Evaluation of New Technologies

RFP Section E, pages 5-6, SOW 8.2.3, page 6

The MAR Team has the expertise and capabilities available to evaluate new technologies as they relate to the NRC specific workforce, processes, and existing technologies. New technology evaluation occurs in direct response to a COR request and may become part of requirements derived by the target ESA and associated Transition Plan. Regardless of why a new technology is evaluated, the results are collected and can be assessed by the ESA for relevance and possible inclusion in the target ESA. This may also support potential business solutions. For more information regarding the proposed ESA maturity lifecycle activities please refer to Figure 14 in Section 1.A.6.2, NRC ESA.

The MAR Team will leverage facilities such as CACI's Cyber Labs (CLs) to evaluate new technologies by simulating certain aspects of the NRC environment. We will also evaluate the stated capabilities of specific vendor tools or solutions, and identify positive and negative impacts to the NRC at both the system and enterprise level. We propose establishing a quarterly roundtable discussion on new technologies at our Team member's cyber lab facilities. This may include the identification and demonstration of new products or technologies.

Our Team has previously supported comparable multiple product research and selection efforts for the NRC Cyber Security Program, such as the automated compliance effort involving product research and tool selection analysis associated with selected vendors including Tenable, nCircle, and ThreatGuard, who offer tools that could play a role in supporting the strategic initiative. Tests were conducted for each of the products to determine the viability of developing in-house templates for automated compliance checks. The final determination was that the most cost effective method was to engage the vendor directly to develop the templates.

When evaluating new technologies we will map each tool to the 18 security families described in NIST SP 800-53 and as outlined in Table 5. This will allow the NRC to fully understand the impact each technology has on the NRC Cyber Security Program and associated security controls.

Table 5. NIST SP 800-53 18 Security Families

• Access Control	• Media Protection
• Awareness and Training	• Physical and Environmental Protection
• Audit and Accountability	• Planning
• Security Assessment and Authorization	• Personnel Security
• Configuration Management	• Risk Assessment
• Contingency Planning	• System and Services Acquisition
• Identification and Authentication	• System and Communications Protection
• Incident Response	• System and Information Integrity
• Maintenance	• Program Management

The resulting analysis will provide the NRC with an understanding of potential return on investment (ROI), as well as how a particular technology potentially solves current challenges, introduces new challenges, overlaps existing technologies, compliments existing technologies, or addresses a combination of these factors. We will add insight and propose recommendations into whether the specific technology has been used by the Federal Government at-large and/or commercial industries, allowing the NRC to determine the risks involved in implementing a particular technology.

1.A.2.4 Analysis of Best Practices

RFP Section E, pages 5-6, SOW 8.2.4, page 6

The MAR Team has the expertise and capabilities available to assess federal and industry best practices for applicability to the NRC processes and culture. For example, over the last six years, we have recommended numerous changes to the NRC's systems authorization artifacts. This includes Security Categorization and System Security Plan templates. We also recommended changes to the overall systems authorization process to allow for parallel efforts in order to meet compressed schedules. We routinely meet with the CSO and staff to discuss areas for improvement to individual artifacts or the security program. With the addition of MAR team members such as CACI, KCG, and Securicon, we will leverage their knowledge from supporting other Federal agencies such as TSA, Intelligence Communities, and DoD to initiate new dialogue such as "Bring Your Own Device," Mobile Computing , Virtualization, and Cloud Computing.

The first step in evaluating a best practice is analysis. Analysis of best practices may occur in direct response to a COR request or as a result of ongoing Cyber Security support efforts across the NRC. This may also support potential business solutions and the ability for the NRC to make informed

decisions or to streamline processes in an effort to reduce costs associated with the development of cyber security artifacts. The MAR Team's analysis will provide the NRC with an understanding of potential ROI, as well as how a particular best practice potentially addresses current challenges or introduces new ones. We will add insight into whether the specific best practice has been successfully implemented by similar Federal agencies, allowing the NRC to fully understand the risks and benefits involved in implementing a particular best practice.

Once the analysis is complete, the MAR Team will provide recommendations through the development and submission of a white paper. The white paper will provide a description of the background or rationale behind developing the white paper, a discussion of potential options for NRC consideration, and a recommended on the course(s) of action. Our recommendations will be based on an understanding of the NRC environment, a sound business case, and represent a positive ROI for the NRC. MAR will offer to provide a briefing or facilitate a roundtable discussion to provide an open forum to address questions or concerns.

The NRC COR will review the white paper and determine a course of action which may include requesting assistance from the MAR Team in incorporating selected recommendations into the NRC Cyber Security Program. The MAR Senior Project Manager, Mr. Evans, will work with the NRC in outlining the engagement of MAR's Technical Team and the associated resources required to fulfill the assistance required from MAR. At this point the activities will be established within the MAR TaskTracker system and monitored under the processes outlined in Section 1.A.1.2.

1.A.3 System Authorization

RFP Section E, pages 5-6, SOW 8.3, page 6

The MAR Team builds upon the investments made to the NRC's Systems Authorization process ensuring that security is addressed throughout all phases of the PMM.

HIGHLIGHTS

- *In 2006, the NRC had only Interim ATOs (IATOs) for their systems*
- *Since 2010 all NRC FISMA reportable systems have achieved and maintained an ATO*
- *MAR currently delivers between 23-30 NRC Cyber Security artifacts per month in support of maintaining ATOs*

The NRC's Office of Inspector General's November 9, 2011 Independent Evaluation of NRC's Implementation of the Federal Information Security Management Act for Fiscal Year 2012 (OIG-12-A-04) states: ***"Over the past nine years, NRC has continued to make improvements to its information system security program and continues to make progress in implementing the recommendations resulting from previous FISMA evaluations."*** MAR is proud to have been a trusted contractor and team player supporting the NRC's leadership and vision over the past six years by assisting CSO, OIS, and the Program Offices in achieving this significant progress in its IT Security Program. Much of this was accomplished by establishing strong working relationships with the CSO, Program Office System Owners and ISSOs, support staff within ICOD, and other contractors providing support to the NRC. Our Team has taken the initiative to truly understand the architecture and purpose of each NRC operational information system. During our current CISSS contract we delivered innovative use of technology and staff to provide the NRC with the combination of skills and knowledge to constantly improve upon our technical work performed.

As part of our approach and solution, we recommend that moving forward we leverage our relationship with NRC System Owners and knowledge of NRC systems to ensure security is addressed at the earliest stages of the System Development Life Cycle (SDLC). Too often, system security is an after-thought. We have seen many cases where attempts are made to retro-fit required security controls into systems after they become operational. Early integration of

information security requirements into the SDLC is the most cost-effective and efficient method for an organization to ensure that its protection strategy is implemented.

1.A.3.1 Obtaining NRC Information Systems Authorization to Operate

RFP Section E, pages 5-6, SOW 8.3.1, page 6

Working closely with the CSO, the MAR Team has developed a standardized approach using NRC templates and guidance. In performing authorization activities over the last six years, we have completed both full packages and "ala carte" activities for discrete portions of the authorization process. This work had provided us insight into resources and schedules required for each type of activity and their applicability within each PMM phase. Through best practices developed under the CISSS contract, the MAR Team proposes a specific Independent Assessment Team to address the testing and evaluation of systems. Members of this team are not involved in the earlier phases of the systems authorization process.

Security Assessment and Authorization activities, from the initial Security Categorization through receiving an ATO, are reliant upon the implementation of 1) a sound, repeatable process 2) tools that automate the process, organize its activities, and support the successful attainment of Authorization, and 3) the capture of metrics (management and technical quality) to be used for program and process improvement – also known as lessons learned. We have taken the time to carefully capture this understanding from lessons learned within the MAR PMOS. This repository of information is used to constantly improve processes, procedures, and enhance the service the MAR Team provides. Examples include improvements to Security Categorization templates, as well as the development of checklists and documentation guidelines for consistency in artifact development.

Increasingly, agencies are adapting a new approach to authorizations that align with the emergence of the new NIST Risk Management Framework (RMF) outlined in NIST SP 800-37, as shown in Figure 9.

It provides a mechanism for agencies to implement an efficient and effective program for managing risk to the enterprise. The NIST RMF serves as the basis for executing the new "C&A" process which is now called the Security Assessment and Authorization (SA&A) process. The MAR Team has worked closely with the NRC's CSO to integrate the RMF into NRC processes which have been used for recent NRC System Authorizations.

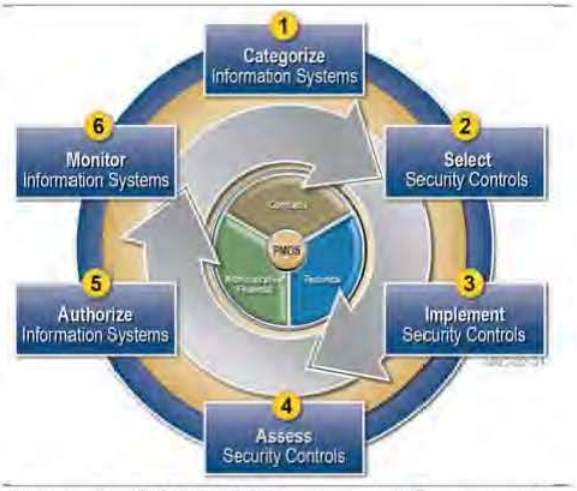


Figure 9. NIST Risk Management Framework.

Figure 10 illustrates the MAR Team's activities under the first five steps of the RMF for supporting the NRC's systems authorizations. Under each RMF step the associated deliverables/artifacts that will be produced under the CSPSS project along with the complimentary components from MAR's PMOS is outlined. Please note that step 6 of the RMF is addressed in Section 1.A.4, Continuous Monitoring.

Throughout the Systems Authorization process, the QA Team will provide oversight and upon completion will conduct a lessons learned meeting. This information will be captured and input into PMOS or the appropriate NRC repositories.

Figure 10. MAR Team System Authorization Process Aligned with NIST RMF. NIST RMF integrated with MAR's PMOS to deliver a repeatable, consistent, and efficient approach to FISMA compliance for the NRC.

E-Authentication Risk Assessment

SOW 8.3.1, pages 6-7

Electronic authentication (E-Authentication) is the process of establishing confidence in user identities electronically presented to an information system. The criticality of implementing appropriate remote authentication solutions, commensurate with associated risk, cannot be over-emphasized. In our experience, E-Authentication Risk Assessments are commonly treated as an after-thought at many organizations. We have witnessed in these other organizations many cases where authentication assurance levels have been incorrectly determined – rendering an application, and its data, susceptible to exploitation.

- *Lead Security Analyst(s) are assigned based on knowledge with the System.*
- *Will serve as a more effective liaison between the Program Office and the CSO to ensure effective communication is maintained throughout the process.*
- *Leverage our in-depth NRC knowledge and understanding to more accurately assess impacts to the NRC's business and mission.*

The MAR Team has assisted in the assessment of over 100 systems to determine the necessity of E-Authentication Risk Assessments over the past six years. We have worked closely with the NRC CSO in determining when the E-Authentication Risk Assessment is required and how it is incorporated into the Security Categorization process. As a direct result of this collaboration, we have assisted the NRC with updating templates for the purpose of simplifying guidance, as detailed in OMB M-04-04, and minimizing subjectivity during E-Authentication Risk Assessments. The E-Authentication Risk Assessment is now incorporated as a section of the Security Categorization report.

Security Categorization Package

SOW 8.3.1, page 7

The MAR Team currently conducts a security scoping interview to determine the proper system or applications classification and impact consistent with NRC guidance, FIPS 199 and NIST SP 800-60. Systems are categorized with a system impact of Low, Moderate, or High. We develop a system security categorization report that identifies the system

- *Over 100 Security Categorizations conducted on CISSS contract.*
- *Today's Security Categorizations unit cost is 60% lower than at contract award.*

scope, inter-systems connectivity, the information sensitivity levels of data processed within the system, the privacy impact of the system, and whether it contains Personally Identifiable Information (PII). Electronic transactions (Inquire, Create, Delete, and Modify) and requisite authentication levels are incorporated into the E-Authentication portion of the report (when applicable) and electronic records disposition. The MAR Team also reviews and recommends changes to the NRC completed privacy impact assessments for consistency with Section 208 of the Electronic Government Act, and information obtained during the systems Security Categorization. MAR will continue to use this process in support of the CSPSS project.

The purpose of the security categorization is to define and document the potential impact level or magnitude of harm that can be expected to result from the compromise of information confidentiality, integrity, and availability within an information system. The NIST SP 800-60 is used to map each of the types of information contained within the system. Impact levels are ranked as Low, Moderate, or High for confidentiality, integrity, and availability based on the extent to which an adverse effect is considered to be limited, serious, or severe in nature and based upon the guidance provided by CSO. The potential impact values assigned to the respective security objectives (confidentiality, integrity, availability) are the highest values (i.e., high water mark) from among those security categories that have been determined for each information type resident on the system. The resulting overall security category of the system is determined by applying the high water mark of each of the three security objectives.

The MAR Team determines and documents the security categorizations of the information systems in accordance with the process outlined in NIST 800-60 and FIPS 199 standards. MAR provides facilitation of this process by gathering inputs from the key stakeholders and developing recommendations for the security categorization at Low, Moderate, or High based upon the system's function, as it relates to the NRC's mission, and the information types processed. Our approach is to conduct the security categorization process with an organization-wide mindset to ensure consistency of information type assessments across the enterprise. With this approach in mind, the MAR Team assisted the CSO in creating a draft NRC Security Categorization Approach document in FY11 which is currently under review.

When conducting a security categorization, MAR evaluates and determines the system boundary by reviewing the system network diagrams, analyzing information data types and flows, evaluating system interfaces and interconnections, reviewing system documentation, and plotting undocumented external network interfaces. Conducting this analysis is imperative in determining the appropriate boundary and subsequent information type impact levels as the results of the security categorization process influence the selection of security controls for the system. This analysis provides the support required for proper system categorization and control selection – thereby providing some assurance that the cost associated with control implementation is appropriate.

In our experience, System Owners occasionally over estimate the potential impact to the organization regarding certain events that may jeopardize the confidentiality, integrity and availability of an information system. MAR recommends taking a holistic approach to assess mission and business drivers during the categorization process. This approach advocates the standardization of information types based on impact levels and agency mission. Our experience indicates that standardizing results in consistent categorizations across the enterprise may potentially reduce the cost of implementing security controls. This approach ensures individual information systems are categorized based on the mission and business objectives of the organization.

Additionally, in conjunction with completing the Security Categorization report, our Team reviews and proposes changes to the system's Privacy Impact Assessment (PIA). The PIA will address 1) what privacy information is being collected, if any, 2) why the information is being collected, 3) the agencies intended use of the information, 4) with whom the information will be shared, 5) what notice or opportunities for consent would be provided to individuals regarding information that is collected and how it is shared, and 6) how the information will be secured.

The Security Categorization will be documented in a report that follows the NRC Template for Security Categorizations. The report will be delivered in draft form and then in final form after NRC comments have been incorporated.

Security Risk Assessment (SRA)

SOW 8.3.1, pages 7-8

The MAR Team understands the full risk management life cycle and the importance of SRAs. This is a vital step in providing the responsible NRC officials with the information necessary to make risk-based decisions in determining the readiness of a system or application for an ATO. Our Team understands a primary goal for NRC is to ensure NRC's IT assets are secure and are able to obtain and maintain an ATO.

- *Leverage our knowledge of NRC requirements, standards, and systems to ensure a comprehensive technical approach to identify the true risk pictures of the system and to consistently map vulnerability assessment tool findings to 800-53 controls.*
- *Proven past performance delivering compliance reviews ensuring detailed and concise documentation that meets necessary assessment requirements.*
- *The use of MAR-developed parsing tools to efficiently map results into NRC specified templates for additional cost savings and accuracy.*

With the movement toward the NIST RMF, the mechanism for aligning security risk to mission objectives with an emphasis on enterprise security risk management is formalized. This approach includes an emphasis on Continuous Monitoring and Continuous Authorizations. To get to that point, a comprehensive security control assessment plan must be developed and executed following NIST SP 800-53A, OMB A-130, FIPS 199, and other Federal and NRC guidance. The results of the security tests and resulting POA&Ms will provide NRC stakeholders, including the CSO, Information Owners, System Owners, and others a baseline to measure readiness for operations or continued operation.

At the foundation of our approach is the understanding of NRC risk tolerance levels and the required security controls within the NRC environment. The MAR Team has gained significant experience and insight by performing Security Risk Assessment activities on nearly all NRC operational systems. In support of the CSPSS project, we will continue to assist System Owners in on-going risk management for existing systems and to prepare new systems for the authorization process. Our experience in developing and executing the SRAs does not guarantee an ATO – ultimately that is dependent upon the status of each system. We have been able to assist NRC System Owners in identifying the full range of risks and mitigation measures in place to create the lowest possible residual risk to the system and to the Agency.

Our Team uses a qualitative Facilitated Risk Assessment Process (FRAP) approach to identify threats and vulnerabilities and to assess the risk exposure. This FRAP approach includes the following activities:

- System characterization including sensitivity of data, data flow, user descriptions and system categorization.
- Review of threats to the system (threat identification).
- Assessment of current and planned security controls (control analysis) using a combination of documentation reviews, interviews, observations, vulnerability scans to determine system configuration and patching levels and penetration tests to assess the boundary protections.

- Provide observations about each control.
- Pairing vulnerabilities with threat-sources.
- Determination of the likelihood (High, Medium, and Low) and impact (High, Medium, and Low) of each vulnerability/threat pairing after factoring in compensating controls and providing statements detailing the determination.
- Assessment of each risk as Low, Moderate, or High based upon the NIST risk-level matrix of threat likelihood and threat impact.
- Development of recommended mitigating controls.
- Selection of mitigating countermeasures for each identified risk.
- Assignment of responsibility for countermeasure implementation.
- Establishment of a timeframe for countermeasure implementation.
- Reporting of results using an NRC-provided risk assessment report template.
- Assist the SO with incorporating and prioritizing the findings into the system's POA&M.

The SRA follows the guidance from the NIST SP 800-30 and NRC Management Directive 12.5. Its purpose is to evaluate and document the extent to which the security controls, are in place and operating as intended, such that the information stored, processed, and transmitted is adequately secured and protected. The risk assessment characterizes system threats and vulnerabilities, including the likelihood of each threat-source exploiting the associated vulnerability, and then determines the potential harm or impact each threat/vulnerability pair and associated threat action could impose upon the confidentiality, integrity, and availability of system information in the event a security control is not properly implemented. The likelihood and the impact associated with a given threat/vulnerability pair is the risk for that particular pair.

The SRA will be documented in a report that follows the NRC Template for SRAs. The report will be delivered in draft form and then in final pre-test form after NRC comments have been incorporated. The SRA is updated and finalized once system testing is completed to reflect validated information.

System Security Plan (SSP)

SOW 8.3.1, page 8

The protection of a system must be documented in a SSP. The purpose of the SSP is to provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements. Description of the information system (including system boundary) and documenting the description in the SSP is required per NIST SP 800-37. A system's ATO is based on an assessment of management, operational, and technical controls.

For the system description, the MAR Team uses the information contained within the Security Categorization and ensures the information systems are thoroughly documented. We will also:

- Identify all planned and existing security controls and document them within the SSP.
- Check that all known security threats, vulnerabilities, and weaknesses in the security controls are identified and documented in the SSP.
- Make sure the status of each control is accurately depicted (in-place, planned, not-planned, not applicable or inherited from another NRC system).
- Make certain that inherited controls are actually in-place by the providing system and an agreement exists between the control provider and the SO of the inheriting system.
- Perform the initial risk assessment with all system stakeholders to identify the current risk exposure of the information system and the current state risk exposure and update the impacted controls in the SSP.

- Ensure the SSP is updated to reflect the results of any recent changes including possible changes to the system's boundary, implementation of new common/inherited controls, findings from security tests or closed POA&Ms.

With the PMM, the SSP must be in place and/or updated in the Elaboration, Construction, and Transition phases in preparation for the development of the System Test and Evaluation (ST&E) Plan. At completion of the testing, the SSP is updated to reflect any modifications to the controls. The SSP is then included in the package for systems authorization.

The SSP is an essential component of IT risk management. The MAR Team understands the need to have this document accurately reflect the system security posture and that the security controls selected are baselined according to the expected impacts to Confidentiality, Integrity, and Availability of the system. For the past six years, the MAR Team has assisted NRC System Owners with the preparation and maintenance of SSPs and has played an integral part in the maturity of this documentation. As noted in the November 2011 Office of the Inspector General (OIG) report, the NRC "has continued to make significant progress in assessing and authorizing its systems" and "the agency completed or updated security plans for all of the agency's 22 operational systems." No deficiencies were noted by the OIG regarding the agency's SSPs.

The SSP will be documented in a report that follows the NRC Template for SSPs. The report will be delivered in draft form and then in final pre-test form after NRC comments have been incorporated. The SRA is updated and finalized once system testing is completed to reflect validated information.

Preliminary Assessment Report

SOW 8.3.1, pages 8-9

- *MAR maintains a Vulnerability Recommendations Library (VRL) to aid in the evaluation of scan results.*
- *There are currently over 600 entries in the MAR VRL.*

As part of the authorization process, the MAR Team performs vulnerability scanning as required by NRC. We have an experienced scanning team in place familiar with the tools and procedures required to efficiently conduct scanning of systems with minimal disruption to daily system operations. Each of our scanning team members has current approval and authorization from the NRC Project Officer and other NRC management. MAR has developed and continually updates a "Vulnerability Recommendations Library" (VRL) within our PMOS. The VRL contains non-sensitive and non-system specific data that assists the scanning team in the evaluation of findings and development of recommendations that are incorporated into the Vulnerability Assessment Report (VAR).

Automated scanning and manual testing determines if the system is concurrently patched and properly configured, operated, and maintained correctly and in accordance with NRC policy and standards. Additionally, these tests help determine whether security controls are operating as intended and validate whether NRC systems continually meet federally mandated and NRC defined security requirements. In performance of the scans the MAR Team will utilize a variety of NRC approved testing tools. Some of the tools and guides we currently use include: nCircle, Nessus, Core Impact, DISA Gold, Air Magnet, Hailstorm, CIS Benchmarks, Microsoft Baseline Security Analyzer (MBSA), and ThreatGuard for United States Government Configuration Baseline (USGCB) checks to conduct the assessment. These are either manual or automatic, and include proprietary and modified open source.

We will use our experience at the NRC and expert-level knowledge of NIST SP 800-53, FIPS 140-2, NRC Management Directives, Committee on National Security Systems issuances (where applicable), and various NRC policies, processes, standards and Organizational-Defined Values to conduct preliminary assessments. The tools and/or specifications are used to assess vulnerability and hardening status for the NRC system hardware, software, and network devices. The VAR

provides the collective findings of these various types of scans and hardening checks, along with recommendations for addressing each finding. Whenever possible the analysts who produce the VAR conduct additional research to identify the specific patches or configuration settings that are recommended to correct the vulnerability, with special attention paid to critical level findings. Recommendations for possible deviation requests are also included where appropriate.

The VAR is developed by the scanning team and reviewed by the QA Oversight Team for submission to the NRC System Owners and other stakeholders for review. We remove false positives from the report. As new findings arise, we add them into our VLR for future reference.

We incorporate an assessment strategy that includes, but is not limited to, the following activities:

- Identifying if the system is vulnerable to any published exploits.
- Determining whether implemented cryptography is currently FIPS 140-2 validated.
- 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.
- Validating the system adheres to Federal regulations, guidelines, and standards.
- Validating the system is hardened per NRC standards.
- Analyzing if the system's implementation adheres to the vendor's recommendations.
- Verifying the systems' procedural controls are adequate.
- Determining if the system's managerial controls are sufficient.
- Observing NRC employees', contractors', and vendors' adherence to policy and procedures.

Upon conclusion of the preliminary testing, the MAR Team documents the results and observations of the tests in a VAR. Findings identified in the VAR will include the following items as outlined in the SOW: Risk Number, Description of Risk, Type of Risk, Associated Controls, and Actions Required or Performed.

MAR also includes the following items to the VAR to assist System Owners in understanding the full scope of the vulnerability:

- Affected Hosts – components (servers, work stations, network devices, etc) that have the vulnerability.
- Vulnerability ID – tool/standard/benchmark used to identify the vulnerability (NRC Standard ID, nCircle ID, DISA Vulnerability ID, CIS Benchmark ID, etc.).
- Status – used to identify if vulnerability is associated with an existing POA&M or result in a new POA&M, an existing Deviation or result in a new Deviation.

Upon execution of testing, the MAR Team performs daily out-briefs with NRC personnel through oral or written status reports. These out-briefs detail the day's testing activities, high level findings, any issues that have occurred, and the plans for the next day's testing. At no time does the MAR Team make decisions without properly consulting with the NRC and receiving the approval on how to proceed. We work with the ISSO and system administrator to conduct initial remedial actions to correct the deficiencies prior to finalization of the SRA, ST&E Report, and POA&M. Any findings that are remediated during the process will be re-tested and validated for proper remediation to an acceptable level of risk. A final copy of the VAR is provided in the completed authorization package. The MAR Team immediately reports all exploitable deficiencies found in the system to the COR.

The MAR Team coordinates and executes all applicable site access and non-disclosure agreements and authority to scan forms with parties other than the NRC prior to commencement of the above mentioned activities, ensuring that project schedules are not impacted.

The VAR will be documented in a report that follows the NRC Template. As this document is part of the independent assessment, it will be delivered in secured read-only PDF format.

Systems Test and Evaluation (ST&E) Plan

SOW 8.3.1, pages 9-10

Through our various contracts with the Federal government, the MAR Team has gained significant experience and insight by performing ST&E activities on nearly all types of operational systems and applications within most operating environments. We bring this expertise to assist the NRC in maintaining their ATOs for existing systems and to aid in new systems achieving an ATO.

We have performed over 50 ST&E activities during the past two years across a wide range of systems and applications. This experience has resulted in our ability to:

- *Assist system owners in gaining or retaining their ATOs.*
- *Development of automation tools and processes that deliver results at or below planned budgets and within tight time constraints.*

The ST&E Plan is developed in accordance with NIST SP 800-53, NIST SP 800-53A, NIST SP 800-37, NIST SP 800-115 and the NRC ST&E Plan Template. The MAR Independent Assessment Team reviews the SSP and develops detailed test procedures to ensure all IT security functional and assurance requirements are fully tested. The procedures will use the following test methods; examine, interview, inspect, and test, and will contain sufficient detail so that familiarity with the system is not required in order for technically trained assessors to successfully execute the various tests. We will use MAR's parsing tools to do an initial control selection and test procedures population that are based on the system categorization, SSP, along with both NIST guidance and NRC requirements. Through the use of these tools and the information contained in our PMOS we are able to prepare plans in a consistent, repeatable process that saves time and allows our analysts to focus on the evaluation of the system.

The MAR Team has been involved with the full cycle of ST&E for numerous agencies - Intelligence Community, NIH, DoD, and TSA - to name a few. Best practices taken from these environments will be brought to NRC Security Management as part of efforts to improve the efficiency of security testing processes. The ST&E Plan identifies all testing assumptions, constraints, and dependencies and includes a proposed schedule that identifies which personnel, hardware, software, and other requirements that must be met for each portion of the schedule to accomplish full system security testing. The following criteria are used: Examine, Interview, Inspection, and Test.

For NRC-common controls and controls inherited from another system, we will verify that the inherited system's SSP is documented that the inherited controls were in-place, and functioning as expected. Our Team works with the NRC to recognize those controls that are inherited from other systems. We also work to continually update and improve ST&E Plan processes and templates and follow the latest process that is in alignment with any existing NRC templates.

The primary objective of the ST&E Plan is to provide sufficient details of the ST&E engagement so that all stakeholders have an opportunity to review, modify, and/or approve the Plan prior to the commencement of actual testing. The MAR Team does not proceed with systems testing until both the System POC and CSO have approved the ST&E plan. The ST&E Plan describes the purpose and scope of testing along with any assumptions, constraints or dependencies. The constraints are particularly important as they detail the controls that will not be tested during the engagement and the reason why. With this, CSO and other stakeholders may decide to postpone the test or perhaps suggest alternative testing methods. Also, the Roles and Responsibilities section of the ST&E Plan clearly defines the role each stakeholder plays in a successful test engagement. There have been situations where testers were not able to fully meet the objectives of the ST&E exercise. If each stakeholder understands his/her role and the

ST&E Plan has been adequately communicated, this type of situation can be minimized, ultimately resulting in delivery of test results on time and within budget.

The ST&E Plan will be documented in a plan that follows the NRC Template for ST&E Plans. The plan will be delivered in draft form and then in final pre-test form after NRC comments have been incorporated. The ST&E Plan may be updated and finalized once system testing is completed should the need to arise perform additional tests that were outside of the original scope of testing. For example, new components are discovered during scanning that would then need to be tested.

Security Control Testing

SOW 8.3.1, page 10

The MAR Independent Assessment Team performs Security Control Testing services in accordance with NIST SP 800-115 and the approved ST&E Plan. The MAR Team's approach is to conduct validation testing that uses multiple vulnerability testing tools and utilities. Inclusive in our approach for standardization is the generation of specific and repeatable test cases for three different types of security testing; 1) Compliance Testing, 2) Best Practices, and 3) Vulnerability Testing. The MAR Team test cases are built on security requirements as defined in NIST SP 800-53A in accordance with NRC security standards, policies, and common controls guidance. Test cases are developed based on best practices from NIST, IT security procedural guides, and leading security industry organizations including the Center for Internet Security (CIS) and the SANS Institute and will be accomplished through interviews, documentation reviews, or testing. Our Team will work with the appropriate government facilitator to verify concurrence of our test cases prior to executing the test. Additionally, in situations where cryptography is required, tests are conducted to determine whether the implemented cryptography module is currently FIPS 140-2 validated.

The security assessment is used to validate overall effectiveness of the confidentiality, integrity, and availability safeguards in place. The assessment validates the implementation and documentation of the safeguards and assesses their ability to properly protect the sensitivity requirements of the system as defined in the SSP. The assessment execution is based on the parameters defined in the Security Assessment Plan. Each test case is executed in a controlled environment and the results are documented and compared with the expected results identified in the test case. Discrepancies between intended and actual results are documented and assigned a severity level based on the increased level of network and/or system risk. At the completion of testing, the ST&E report, VAR, and POA&M are completed to properly document results.

The MAR Team coordinates and executes all applicable site access and authority to scan forms with parties other than the NRC prior to commencement of the above mentioned activities.

The Security Control Testing will be documented in a report that follows the NRC Template for Security Control Testing. As this document is part of the independent assessment, it will be delivered in secured read-only PDF format.

POA&M Report

SOW 8.3.1, page 11

The requirement for government agencies to maintain POA&Ms began under the oversight of the GAO and Congress. OMB provides detailed reporting roles and responsibilities, minimum information assurance performance measures, and reporting formats in detailed memorandum instructions. POA&Ms are required under FISMA of 2002 and related requirements are refined through annual OMB FISMA reporting instructions.

POA&Ms are used to identify and track known information security weaknesses. These documents detail the plans and proposed implementation by the ISSO and include the resources required to accomplish corrective actions, the personnel responsible for mitigating weaknesses, the milestones supporting mitigation, and the scheduled dates for completion of all required actions. Adequate POA&M documentation defines priorities for resolving issues, supports the justification for and allocation of resources, provides accurate statistics for submission to OMB, and provides a centralized information source for staff, managers, administrators, and officials involved in the process. POA&M components include:

- Weakness ID
- Issue Date
- Weakness Description
- Point of Contact
- Risk Level
- Additional Resources Required
- Funding Availability
- Scheduled Completion Date
- Brief Description of Work/Services
- Milestones with Completion Dates
- Changes to Milestones
- Source
- Date Closed
- Status.

Our Team assists the NRC Program Offices with the documentation of their systems' weaknesses through prioritization recommendations and technical guidance. We upload all POA&Ms created from the authorization process into Xacta for tracking and reporting purposes.

Contingency Plan (CP)

SOW 8.3.1, pages 11-12

The MAR Team will continue to support the NRC staff in the development and documentation of a CP and test procedures in accordance with federally mandated requirements, NRC defined cyber security requirements and contingency approach. The System CP is documented in a report that follows the NRC Template for the System CP. The Plan is maintained in its hard copy form for contingency execution should the NRC Network Infrastructure be unavailable. The MAR Team uses checklists, accessible to the team in the PMOS, that were developed from experience gained over the past four years to make certain we are following a consistent and repeatable process in developing CP Plans.

The Disaster Recovery and Reconstitution Procedures discuss the process to restore the information system or components to a known state and define the actions taken to test and validate system capability and functionality. Tabletop exercises are a good starting point from which specifics can be documented and tested until an effective plan is achieved.

The Business Impact Analysis (BIA) is a key step in the contingency planning process. The BIA enables the system owner to characterize and correlate system components with the critical mission/business processes and services to determine contingency planning requirements and priorities should a disruption occur in the system.

We will use the CSO-approved template to create the BIA document and work with System Owners to identify critical mission/business processes to determine the maximum allowable outage times the NRC can tolerate while still maintaining the mission. During this process, a thorough evaluation of the critical resources necessary to resume mission/business processes is defined. This will allow the NRC to establish priority levels for sequencing recovery activities and resources. The overall result of the BIA is an information system recovery priority hierarchy.

We also provide detailed procedures for the Notification/Activation Phase, Recovery Operations, and Return to Normal Operations sections. There may be situations where the CP must be executed by contractors who are unfamiliar with the system. Procedures must be sufficient so that

any technically trained individual can successfully follow the procedures. To that end, it is critical that the CP contains detailed information regarding:

- Notification procedures including a list of all stakeholders with applicable contact information.
  - Stakeholder contingency roles and responsibilities are also included in this list.
- A current list of equipment (hardware and software) comprising the system including Baseline Configuration information (O/S levels, configuration settings, etc).
- Location of the system's standard operating procedures.
- Identification of any systems that the system is dependent upon including contact information for the dependency system.
- References to the emergency management plan and occupant evacuation plan.
- References to the appropriate continuity of operations plan.

The CP will be documented in a report that follows the NRC Template for CP. The report will be delivered in draft and then in pre-test form after NRC comments have been incorporated.

Contingency Plan Test Report

SOW 8.3.1, page 12

Over the past two years MAR has prepared 50 Contingency Test Reports covering over 30 systems.

Our Team provides 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 will follow the procedures developed and documented in the CP. We will document the testing in a System CP Test Report. The CP Test Report will be developed in accordance with federally mandated requirements, NRC defined security requirements, NIST SP 800-34 "Contingency Planning Guide for Federal Information Systems", NIST SP 800-37 "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle", and the NRC Contingency Test Report Template.

The CP Test is documented in a report that follows the NRC Template for NRC Contingency Test Report. The CP Test Report identifies all testing assumptions, constraints, and dependencies, as well as any anomalies, impromptu tests, and deviations encountered during testing. The CP Test Report includes the actual testing schedule, detailed test results for each test procedure outlining specific errors encountered, and a table of test findings incorporating any test issues and recommendations. The CP Test Report identifies any problems encountered during testing and the resulting action items for the system. The CP Test Report is delivered in draft and then in final form after NRC comments are incorporated. The MAR Team will update the system's CP once the CP Test Report is completed to reflect validated information.

Authorization Package

SOW 8.3.1, page 12

MAR has supported 19 System Authorizations since FY 2010.

Our Team will provide the final security accreditation package which includes the Security Categorization Package (including the E-Authentication Risk Assessment if necessary), SRA, Preliminary Assessment Report/VAR, SSP, ST&E Plan, ST&E Report, POA&M, Deviation Requests, CP, CP Test Report, and ATO memo to the System COR for review and submittal to CSO. The MAR Team will also work closely with the government CISO and the DAAs to answer questions that may arise about the system, the POA&Ms, Deviation Requests, or overall residual risk. Packages are assembled in a manner to provide the DAA with the essential information needed to make certain that systems are operating at an acceptable level of risk to the NRC.

The MAR Team will work with the Senior Information Security Officer and provide a recommendation on the residual risk of the system and the impact on mission processes. All risk analysis is conducted in accordance with the Risk Management Strategy.

Supporting Documentation

SOW 8.3.1, pages 12-13

We will identify and develop any necessary documentation (standard operating procedures, service level agreements, memorandums of understanding, interconnection agreements, etc.) that supports NRC's information security programs and initiatives so that the system is prepared to engage in the full authorization process. All documentation will be developed using existing NRC templates and will provide overviews for the information security program and detailed instructions for using and operating applications and tools. This documentation will be developed to ensure it has addressed all federally mandated and NRC defined cyber security requirements. Processes and procedures will include baselines and metrics for measuring the effectiveness and quality of the information security program. All documentation will undergo a quality control review, as described in Section 1.A.1.1, to ensure it is technically and grammatically correct before delivery to the NRC.

MAR has a proven record of accomplishment for providing this type of support to the NRC. MAR's involvement in creating supporting system documentation for the HSPD-12 authorization effort was instrumental in keeping the project on schedule. The result was a successful ATO in 2010.

1.A.3.2 Obtaining Laptop Authorization to Operate

RFP Section E, pages 5-6, SOW 8.3.2, page 13

As laptops processing data are required to comply with all federally mandated and NRC defined cyber security requirements, the NRC requires that laptop systems obtain a Laptop ATO prior to processing any information. The MAR Team has supported the assessment of over 80 laptops at the NRC. We have approached each effort as an opportunity to partner with the various NRC Offices to review the established ATO process, find efficiencies, and improve the process during each assessment. Over the course of our work to-date, we have been able to cut the cost of performing these assessments by 20% through lessons learned and by working with the Program Offices to coordinate the ATO effort in a more efficient manner.

The MAR Team approach to the Laptop ATO Authorization effort consists of three steps:

- **Step 1** – If requested, we provide technical support to patch the laptops for both operating system and application patch compliance. The staff member performing this support is a member of the integrated project team and is not involved in the assessment of the laptop system.
- **Step 2** – A member of the MAR Independent Assessment Team assesses the configuration of the laptops against both federally mandated and NRC defined cyber security requirements. This includes using an NRC authorized tool to ensure compliance with the U.S. Government Configuration Baseline (USGCB), a patch compliance check and a manual check of the laptop configuration based upon the CSO Laptop Minimum Security Checklist.
- **Step 3** – The Independent Assessment Team member documents the laptop system by using the CSO's Laptop Certification Transmittal Memo Enclosure.

When completed, the Laptop ATO package consists of the following deliverables:

- **Laptop Certification Transmittal Memo** – The formal submittal memo that accompanies the Transmittal Memo Enclosure when submitted to CSO and the Office of Information Services (OIS) for review. This document serves as the formal request to review the Laptop ATO package.
- **Laptop Certification Transmittal Memo Enclosure** – Provides high-level information about the laptop system. It includes brief descriptions of the laptop system's characteristics, the roles and responsibilities of laptop system personnel, a system inventory (including the hardware and software of each laptop) and other pertinent information.
- **Laptop Minimum Security Checklist** – A Microsoft Excel spreadsheet that specifies specific minimum-security requirements that the laptop assessor must verify for each laptop. The checklist consists of three columns. The first column is the "Requirements" column that

describes the specific security requirements that need to be verified. This column is part of the template and does not require any additions or modifications by the assessor. The second column is the Pass/Fail column. The assessor completes this column as Pass, Fail, or Not Applicable (N/A) based on the findings of the assessment. If the requirement is assessed as either Fail or N/A, the assessor provides a brief explanation in the third column describing why the laptop system fails to meet the requirement, or why the requirement does not specifically apply to the laptop system.

These deliverables vary slightly depending on the type of laptop system being assessed (General, SGI or Classified) as the requirements that each type of system must comply with on the Laptop Minimum Security checklist may differ.

Throughout the Laptop Authorization process the QA Team will provide oversight and upon completion will conduct a lessons learned meeting. This information will be captured and input into PMOS or the appropriate NRC repositories.

1.A.4 Continuous Monitoring Support

RFP Section E, pages 5-6, SOW 8.4, page 13

As systems within the NRC have obtained their respective ATOs, the MAR Team has worked and will continue to work closely with the CSO in developing and implementing the current Continuous Monitoring process.

HIGHLIGHTS

- *MAR has provided continuous monitoring support to the NRC since FY 2009 and currently supports 15 NRC systems through Continuous Monitoring*
- *The 15 systems are supported by a combination of 3 scanning staff and 4 security analysts who are engaged during the appropriate phases of Continuous Monitoring – all tracked through MAR's PMOS.*
- *We will continue to provide continuous monitoring support for the CSPSS project by using our established processes and related tools currently in place for the CISSS contract.*

As part of an effective Continuous Monitoring Program, risks are not just reviewed annually, but also on an on-going basis as part of a regular process of re-evaluating vulnerabilities and threats. This provides a near real-time view of system risks throughout the system's operational life. It is more effective to continually monitor and maintain the system rather than look at annual snapshots that may not include business environment changes, new vulnerabilities, new attack vectors, or changing threat sources as a result of a changing business and political climate. Our management team and security analysts have worked hand in hand with both the CSO and other NRC Program Offices to continually improve upon the process through forward thinking and lessons learned from each continuous monitoring task. The current process in place addresses federally mandated and NRC-defined security requirements. The process also supports the NRC Program Offices with the development of their Information Technology Security Risk Management (ITSRM) activities and assists the CSO with reporting the accurate status of continuous monitoring program activities to the Office of the Inspector General (OIG) and other government agencies.

As shown in Figure 11, the MAR Team will support the NRC and its Program Offices in maintaining a continuous monitoring process that meets federally mandated and NRC defined security requirements including those outlined in CSO-PROS-1323, U. S. NRC Agency-wide Continuous Monitoring Program issued in June 2010. Further, we consistently improve the efficiencies of achieving on-going compliance through quarterly lessons learned meetings, both internally and with the Program Offices. This lesson learned information is maintained in MAR's PMOS so that lessons learned from one Program Office may be used to benefit all of the Program Offices supported.

Figure 11. Continuous Monitoring Process.
We will provide Continuous Monitoring support aligned with NIST and NRC guidelines. Activities will be supported by our established management practices and will be overseen by the QA Team.

Mr. Evans, will play an integral part for the on-going development and execution of the Continuous Monitoring process including support of the following specific elements:

- Coordinate the efforts of the CSO, NRC Program Offices, and continuous monitoring support staff on the contract through routine meetings and ongoing correspondence.
- Serve as the primary POC between the CSO, NRC Program Offices, and the MAR Team.
- Closely manage the task's constraints (cost, time, and scope) with the assistance of Ms. Quivey and the MAR QA Oversight Team.
- Apply knowledge, skills, tools, and techniques to contract activities to meet/exceed expectations.
- Work with the NRC Program Offices to ensure residual risks to their systems are minimized.
- Assist the NRC Program Offices in establishing their continuous monitoring schedules so federally mandated and NRC defined security requirements are met.
- Report any circumstances that might impact the ability of the MAR Team to meet the stated objectives of these tasks to the NRC COR and each NRC office's representative.

The Continuous Monitoring program addresses the following areas of involvement, each of which is supported directly by the MAR Team as described in the subsequent paragraphs:

- Support to the Program Offices for the coordination of their continuous monitoring requirements.
- Annual Security Controls Testing.
- Quarterly System Scanning and Reporting.
- Resolution and Quarterly updating of the POA&M in Xacta.
- Annual support of Contingency Planning and Testing.
- Annual update of the SRA and SSP.
- Security Engineering Support.
- Updating other system documentation as needed (memoranda, agreements, procedures, etc.).

Throughout each phase of the continuous monitoring process, the QA Team will provide oversight and, upon completion of deliverables, will conduct a lessons learned meeting. This information will be captured and input into PMOS or the appropriate NRC repositories.

Coordinate Continuous Monitoring Efforts

SOW 8.4, page 13

The MAR Team works closely with the SOs, ISSOs, and CSO in coordinating continuous monitoring activities. Over the past six years, we have gained the in-depth knowledge of the required security risk management activities and the posted schedule of these activities for each NRC system. Continuous Monitoring activities will be planned and scheduled to minimize the impact on daily

operations. The MAR Team will provide additional insight into the overall risk posture and serve as a clearinghouse for the ongoing evaluation of risk. In this role, we conduct trending and root cause analysis of this information to provide NRC with risk information that facilitates more dynamic and informed risk management decisions in securing key information assets.

We will use a FISMA Compliance Plan in order to assist the System Owner's representatives with the establishment of their continuous monitoring schedules. The FISMA Compliance Plan provides specific dates and milestones for Annual Security Controls Testing, Quarterly Scanning, POA&M Reporting, annual Contingency Planning and Testing, and annual SRA and SSP updates.

As a part of our approach, we will continue to incorporate lessons learned to improve the efficiency and effectiveness of continuous monitoring efforts by using a standardized approach methodology to leverage baseline test results for further improvement. This approach allows us to efficiently use existing assessment information and POA&M data to reduce the level of effort in redundant testing activities, especially for more static controls (e.g. documentation, policies, procedures, etc.) that do not change as frequently. Following this process, we will be able to maximize the cost efficiency and stay within budget.

Perform Annual Security Controls Testing

SOW 8.4, page 13

Under the current CISSS Contract, MAR has completed an average of 22 ASCTs per year over the past four years.

The MAR Team conducts Annual Security Control Testing (ASCT) of the NRC's information systems according to NIST SP 800-53A "Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans". We ensure that all test cases and assessment plans account for the discrepancies between NIST SP 800-53 and NIST SP 800-53A and the development of custom test cases to address all controls as required. From our current NRC work, our QA Team has developed a series of ASCT checklists and standard criteria for use by our technical team in the testing and development of ASCT reports that are used to provide consistent delivery artifacts to the NRC stakeholders for their review and evaluation.

The selection criteria are based upon those factors set forth by the CSO, federal guidance, common and inherited controls, and each system's POA&M items. Additional selection criteria may also include, at a minimum, sensitivity level of the system, the requirement to test volatile controls, and controls identified for annual testing. Each fiscal year our Team performs a comprehensive assessment of the selected management, operational, and technical security controls for each system. The assessment determines the extent to which each system's controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting federal guidance and NRC defined security requirements. Upon completion of testing we develop an ASCT Report for each system and incorporate any findings into POA&M Reports.

Test plans go through proper vetting within CSO and the various Program Offices. For instance, the control selection process, as part of annual security control testing, can be quite dynamic – depending upon emerging threats, maturity of NRC-provided controls and changes to a system's security posture. After coordination with the System Owner, the ASCT Plan will be submitted to CSO for final approval. During this vetting process, the testing of additional controls or special test cases may be requested, and whereby the plan is updated accordingly.

The draft ASCT Reports and the POA&M Reports are submitted to the NRC Project Officer, System Owner, and ISSO for review and comment. The MAR Team revises and updates each deliverable as appropriate and provides final versions. The final reports are also provided to the ESA Team and assessed as part of holistic ESA analysis. We will continue to apply this same proven methodology in performing future Security Controls Testing.

Conduct Quarterly Scanning

SOW 8.4, page 14

MAR has an experienced scanning team in place that is ready to perform under the CSPSS project. This team is familiar with the tools and procedures required to efficiently conduct scanning of NRC systems with minimal disruption to daily system operations. Each of our scanning team members has a current approval and authorization from the NRC Project Officer and other NRC management personnel. We understand the processes for preparing and submitting scanning approval forms and emails prior to commencement of scanning activities.

- *Trained, certified, and NRC authorized scanning team.*
- *Support in the creation of NRC procedures required to efficiently conduct scanning of systems with minimal disruption to daily system operations.*
- *MAR-developed parsing tools for document creation.*
- *MAR-developed scanning tools for expediting manual checks.*
- *MAR-developed VRL knowledge base with over 600 entries.*
- *Scanning team is "assigned" systems so they are familiar with the system and administrative staff. This reduces the learning curve when scanning the system.*
- *Expertise with XML to generate custom reports from the raw data scans.*

The MAR Team incorporates an assessment strategy that includes the following activities:

- Identifying if the system is vulnerable to any published exploits.
- Determining if the system has the latest patches installed.
- Determining if the system is using any unsupported hardware/software.
- Analyzing if unnecessary ports or services are available.
- Verifying the system adheres to Federal regulations, guidelines, and standards.
- Validating the system adheres to NRC hardening requirements.
- Identifying if SANS top 20 or vendor-identified vulnerabilities are present in the system.
- Analyzing if the system's implementation adheres to the vendor's recommendations.
- Determining if the system's managerial controls are sufficient.
- Observing NRC employee, contractor, and vendor adherence to policy and procedures.

As previously stated in Section 1.A.3.1, MAR developed and continually updates the VLR within our PMOS. The VRL contains non-sensitive and non-system specific data that assists the scanning team in the evaluation of findings and development of recommendations that are incorporated in the preliminary Findings Tracking Sheet (FTS) and Quarterly Scanning Report (QSR).

Quarterly vulnerability scanning establishes whether or not the system's security controls are operating as intended and ensure that systems continually meet federal guidance and NRC defined security requirements. All risks determinations will be measured according to NIST SP 800-30 "Risk Management Guide for Information Technology Systems" using the defined Risk-Level Matrix. Figure 12 provides MAR's Quarterly Scanning Process and the associated phases. The six phases for quarterly scanning are:

- **Phase 1: Preparation** – 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** – Conduct scans, review documentation, and interview personnel to collect needed information to perform a risk analysis of the organization's systems.
- **Phase 3: Draft Assessment Reports** – Develop System Assessment Reports that identify the risks each system poses to itself, its data, and the NRC infrastructure.
- **Phase 4: Validate Findings** – Validate findings, ensure risks have been properly assessed, and develop mitigation strategies that will address deficiencies in consultation with the System Owner, ISSOs and System Administrators.
- **Phase 5: Finalize Assessment Reports** – Incorporate NRC's comments into the Assessment Reports and deliver the final version of the Assessment Reports to the COR.
- **Phase 6: POA&M Report Updates** – Incorporate any findings into each system's POA&M report.

Figure 12. Quarterly Scanning Process.
The MAR Team's Quarterly Scanning Process is broken into six phases to include the associated activities to routinely assess system security controls.

When performing the scans, the MAR Team will continue to use a variety of NRC approved manual and automatic testing tools (nCircle, Nessus, Core Impact, DISA Gold, Air Magnet, Hailstorm, ThreatGuard, etc.), and MAR developed and modified open source applications to conduct the vulnerability scanning in accordance with CSO approved quarterly scanning procedures.

The initial FTS is developed by the scanning team and reviewed by the MAR QA Team for submission to the NRC System ISSO for review and comment. MAR reviews system documentation to ensure that findings that are previously known false positives or approved waivers are not included in the FTS. We recommend a meeting occur between the scanning team, ISSO, and system administrators to review the FTS prior to commencing remediation efforts. We have found this type of meeting to be invaluable as it can clear up confusion as to what a finding means, how it may be remediated, and/or why the finding is valid. At the end of a 30 calendar day findings remediation period, the MAR team will perform a remediation validation. Validation will be performed in the most cost efficient manner possible. For example, it may suffice that a simple screen shot closes out a manual check finding. Once all final checks are performed, the results will be documented in a formal QSR. All QSRs must be accepted by the NRC Project Officer, the System Owner, and ISSO. We will revise and update each deliverable as appropriate and provide final versions to the NRC. As new findings arise they will be added into our VRL for future reference.

Update POA&M Reports

SOW 8.4, pages 14-15

POA&M updates are provided quarterly in accordance with the CSO POA&M process and checklist and are updated to reflect the current system security posture. Any new vulnerabilities discovered are added and assigned to the appropriate system. Our Team will continue to assist the NRC Program Offices with the resolution of their POA&Ms through technical guidance, documentation review, recommendations, and updating. Revisions of the POA&Ms will be performed quarterly in Xacta (CSO FISMA Compliance automated tracking tool) in accordance with the NRC POA&M process, and provided to the NRC office point of contact two weeks prior to the required submittal to CSO to allow time for review and updating.

The MAR Team will consolidate information collected by Integrated Project Team members supporting the Program Offices, our QA Team, and staff providing CSO POA&M support to clearly outline issues and security concerns. Recommendations will be developed and provided to delineate risk areas and appropriate measures identified to mitigate areas of concern.

Update Contingency Plan (CP)

SOW 8.4, page 15

The MAR Team supports the NRC staff in the update of their CP and test procedures on at least an annual basis to ensure that the system CP information is valid and effective. The system CP is documented in a report that follows the NRC Template for the system CP. The plan is maintained in its hard copy form for contingency execution should the NRC Network Infrastructure be unavailable. We use checklists previously developed from our past work that are stored in and accessible from the MAR PMOS. As changes are made to regulations, the organization, and/or systems, the MAR Team will work with the System Owners to determine if the system CP should be modified. We will continue to ensure that updates to the CP are developed and applied using established procedures in a consistent and repeatable manner.

Develop Contingency Plan Test Reports

SOW 8.4, page 15

Our Team will continue to support the annual testing of the CP. The CP Test is documented in a report that follows the NRC Template for NRC Contingency Test Report. Currently at the NRC, we capture and track the key dates associated with this CP and other Continuous Monitoring activities within the MAR PMOS. As a result, our Team has been proactive in providing NRC stakeholders with sufficient notification as to upcoming milestones associated with their annual requirements for updating and retesting to assist in their planning and budgeting for security activities.

Update SRA and SSP

SOW 8.4, page 15

The update of the SSP and SRA is an essential component of IT risk management. Maintaining these documents ensures that the system security posture is accurately documented as changes to the system are made, and/or as threats, vulnerabilities, technologies, and business requirements and processes evolve.

The SSP must be updated at least annually or within 60 days of significant changes as identified in the NRC ITSRM. Furthermore, the SRA must be updated at least annually to reflect results of continuous monitoring activities and other assessment or review activities. With our institutional knowledge of NRC systems, the MAR Integrated Project Team will update these documents or draft new documents for submission to the appropriate NRC office for review and comment in an accelerated and efficient manner. We revise and update each deliverable as appropriate and provide final versions to the NRC Project Officer, System Owner, and ISSO. As required, we also will assist with the updating of other security related system specific documentation. Changes to the SRA and SSP may stem from continuous monitoring activities, such as ASCT, that identify weaknesses or vulnerabilities that could indicate controls are not operating as intended. The SSP will serve as the authoritative source for the status of each of the NIST SP 800-53 security controls and will be aligned with the Continuous Monitoring activities.

Provide Security Engineering Support

SOW 8.4, page 15

As system changes occur, the MAR Integrated Project Team provides security engineering support to verify and validate proposed architectures and implementations based on sound security principles and practices in accordance with NRC guidelines.

In support of NRC's IT security solutions architecture, the MAR Team will provide full lifecycle engineering support for current and future information security solutions. As a part of any defense-in-depth strategy, we understand the importance of ensuring security solutions are operating effectively across the NRC enterprise. Our Team has supported several clients in the

research, planning, deployment, and maintenance of IT security solutions including; intrusion detection and prevention systems, ArcSight and security information management solutions, web proxies, mail proxies, vulnerability assessment solutions (e.g. Foundstone, AppDetective, Hailstorm, WebInspect), asset management, and secure configuration (e.g., SecurityExpressions, BigFix). Our understanding of the NRC security policies, standards, and requirements combined with our knowledge of the operational requirements and potential threat environment and vulnerabilities will assist us in developing an effective and efficient security controls.

We will also work with the System Owner's representative to ensure that all supporting documentation is kept up-to-date. This will be performed in consultation with the CSO to ensure that the documentation is in compliance with the latest NRC approved templates and security requirements.

1.A.5 Data Calls

RFP Section E, pages 5-6, SOW 8.5, page 15

The MAR Team has personnel familiar with the NRC programs, key staff, and the appropriate NRC data repositories and external systems to quickly determine and collect the data from various sources of information.

HIGHLIGHTS

The MAR Team's in-depth understanding of NRC systems and processes will facilitate rapid and accurate response to data calls.

The MAR Senior Project Manager or a MAR designated point of contact (POC) will receive, validate, and respond to data call requests. We will assist the NRC in rapidly responding to data calls and requests for information in support of the Cyber Security Program. These requests may come from multiple sources including the NRC Office of Inspector General (OIG) and other government organizations, and may also include the NRC CSO or other NRC Program Offices. The results of these data calls and metrics are used by the Chief Information Security Officer (CISO) and Cyber Situational Awareness, Analysis and Response Team (CSAART), and FISMA Compliance and Oversight (FCOT) to brief NRC Executive Management, the OIG, ISSOs, key personnel, and possibly other government organizations such as the U.S. Computer Emergency Readiness Team (US-CERT) and other offices within the DHS.

To facilitate rapid and accurate response to the data calls the MAR POC will be the single point of contact for receiving the request, coordinating the collection of information, and preparing the response to the data calls. In this way, we will make certain every request is valid and responded to with the quick turnaround often required for data calls. Figure 13 illustrates the lines of communication for the coordination and flow of activities to rapidly respond to data calls. The MAR POC will be the gateway for the receipt and transmission of information necessary to coordinate the evaluation, research, collection, compilation, and adjudication and response of data call requirements.

Figure 13. Data Call Response Lines of Communication. The MAR POC will be responsible for coordinating and responding to data calls.

Our POC will first verify the data call request is from a duly authorized representative and the information requested is approved for release to the requesting official. The MAR POC will then:

- Determine the data sources to fulfill the data call, which may include systems, data repositories, or personnel from the NRC, MAR CSPSS Team, or external sources.

- Coordinate the collection of data from the identified data sources.
- Compile information and validate that it is complete and accurate.
- Submit the information to the appropriate requesting parties.
- Complete a log of the request including date and time of the request, the requestor, information compiled including the data sources, and the date and time of request close-out.

1.A.6 Cyber Situational Awareness

RFP Section E, pages 5-6, SOW 8.6, page 15

The depth of personnel resources and diversity of technical disciplines within the MAR Team allows us to offer a full-spectrum cyber situational awareness support, as well as the ability to address other challenges that may arise.

The MAR Team understands the constantly evolving nature of the cyber threat environment and the global information assurance operational framework that directly affects the cyber defense posture of the NRC. We will continue our support of NRC Cyber Situational Awareness programs including; incident response efforts, ESA, vulnerability assessments, source code reviews, penetration testing, and security impact assessments. Our Team has significant experience engaging vendors and evaluating vendor technologies to determine how they can support the objectives of the NRC Cyber Security Program. The following Sections present our Team's approach and related experience for addressing the cyber situational awareness requirements in the NRC environment.

1.A.6.1 Incident Response Efforts

RFP Section E, pages 5-6, SOW 8.6.1, pages 16-17

We will continue to support the CSO office to improve the Incident Response (IR) Program through innovative program enhancements and proactive collaboration with OIS and other NRC organizations to ensure the roles and responsibilities of the IR Program are understood.

The MAR Team currently assists the NRC in maintaining their agency wide IR Program in accordance with federally mandated and NRC defined security requirements. Our support will continue to facilitate an efficient and effective IR operation and provide recommendations for continuous improvements including IR planning, procedures, training, testing, monitoring, and reporting to better prevent, detect, respond to, and recover from incidents using on a holistic enterprise analysis methodology.

Our approach exceeds the criteria specified in the SOW. The MAR Team understands the CSO's primary role in the NRC's IR capability entails the coordination of activities both in preparing the NRC to handle incidents and in the actual response to incidents. The IR Team must rely heavily on relationships with several organizations within the NRC to facilitate cooperation and overall program success. During each step, our interaction with those organizations will be fully collaborative to achieve IR current objectives and future program improvements. Our technical approach for the continued implementation of a comprehensive IR Program will be tailored to meet current NRC Management Directives and policy requirements.

Incident Response Processes and Procedures – These efforts will support the development, review/updating, and dissemination of IR documentation. We will work with all stakeholders, including the Security Operations Center (SOC), Help Desk, and System Owners to ensure documented processes and procedures are up-to-date, relevant, accurate, complete, and compliant. The review and finalization of procedural documentation will ensure that staff roles and responsibilities are clearly defined and provide senior NRC leadership with a well-defined set of objectives and activities. We review and update these processes at least annually, as well as in response to post-incident lessons learned findings and ESA recommendations.

Incident Response Training – In support of training requirements, we will continue to re-assess and update IR training materials to ensure they correspond to current established policies and procedures and will support the initial and annual refresher training for personnel. Training curriculum will include the use of actual case studies of closed incidents and have a strong focus on lessons learned, including discussions on the impact of IR cases on response planning and procedures. The training will ensure that staff roles and responsibilities are clearly defined and communicated to support effective response measures in the event of both small and large-scale incidents. The use of multimedia-based training materials, computer-based visualizations, and simulations will enhance the learning environment and automated distance-learning tutorials and training aids will provide increased efficiencies in reaching target students across the organization. We will also provide quarterly awareness e-mail messages and notifications of processes changes on an as-needed basis.

Incident Response Testing and Exercises – In addition to staff IR Training, we plan and facilitate both table-top and live test activities to quantify and document effectiveness of the response procedures and protocols. Some exercises will be announced and coordinated in advance, while others are unannounced to better assess readiness. The staff will have the opportunity to practice their roles and responsibilities and apply the knowledge they learn in training to maximize the NRC's IR readiness. Our Team member, CACI, will provide their Cyber Solutions Lab as a potential launching point for simulated external attacks. All tests will be coordinated through and authorized by the CSO office.

Incident Handling – We will apply our extensive knowledge of, and experience with, the NRC's IT environment to verify reported incidents to qualify and validate the incidents before responding. Once validated, the MAR Team balances two competing goals; the preservation of evidence and the active defense of the NRC's systems. Through the policy, planning, process, and training activities we will make sure the NRC's priorities are clearly identified and communicated. For example, we will immediately begin to coordinate response activities, and perform a full system backup to preserve evidence. If the NRC's priority is for the preservation of evidence, then the backup will take priority; however, if the NRC's priority is recovery, the backup will only be performed if it will not significantly hamper the recovery effort.

Our implementation of IR handling capabilities will be comprised of an integrated set of procedures, tools, and protocols that support the planning, detection, verification, declaration, coordination, response, containment, continuity of operations, and remediation, restoration, and close-out activities. Our Team will also support the NRC continuous improvements in enhanced IR capabilities through our recommendations and developmental support of automated tools for detecting, classifying, tracking, and reporting incidents.

We will rely on our existing NRC relationships, solid and well-communicated procedures, and coordination skills to ensure an incident is quickly contained, any malware is carefully eradicated, and system recovery happens in a timely manner. An incident will not be closed until all impacted IT components are restored, cleaned or disposed of, any evidence is properly collected, and the system is restored to full and validated operation.

Incident Monitoring – From the moment an incident is reported until the incident is determined to be closed, the status will be tracked to ensure timely resolution and closure. Records will be kept of the time/systems involved, observations, and actions performed. We use automated tools such as the RSA-based IR Database tool for both internal and collaborative tracking to enable automated incident information flow between the SOC and the IR Team, build a knowledge base across incidents, and better aggregate incident information for more holistic analysis by the ESA Team.

Incident Reporting – We understand the importance of reporting incidents in a clear, concise, and timely manner to appropriate organizational officials and System Owners. At an appropriate time relative to an incident, we will report any discovered system weaknesses, deficiencies, or vulnerabilities to the appropriate System Owners and officials. This ensures the NRC takes steps to better protect its systems and prevent similar incidents in the future. The MAR Team will also recommend enhanced use of Fidelis and can work with the CSO to conduct additional tool assessments through CACI's Cyber Solutions Lab.

Incident Assistance – IR handling and reporting often requires more than coordination and response in accordance with defined procedures. The use of expert advice from SME resources will be provided to support the handling of security incidents and the identification, qualification, and implementation of new technologies and IR techniques. The MAR Team has the appropriate staff and skills to directly assist NRC staff, including personnel with well-established and demonstrated experience in intrusion detection, incident response, ethical hacking, as well as CISSP, CCNA, CCDA, CEH, CISA, and other certifications.

Incident Response Plan – We will continue to work to ensure the IR Plan is up-to-date, relevant, accurate, complete, and compliant. The Plan will provide a roadmap and organizational structure to support the implementation and continuous improvement of IR capabilities including approach, organizational structure and drivers, incident reporting criteria, response metrics, and areas of future focus. Our Team will also evaluate and update the plan as part of the Target ESA and associated Transition Plan.

1.A.6.2 NRC Enterprise Security Architecture (ESA)

RFP Section E, pages 5-6, SOW 8.6.2, pages 17-19

The MAR Team's ESA approach will provide a framework by which the NRC's Cyber Security Program continuously matures. We will achieve this through a process of iterative lifecycle activities to continuously provide key information enabling constant ESA analysis and incorporating changes into the "As-Is" and Target Architectures. This process will provide rapid visibility into the NRC's current security posture, as well as ongoing insight for necessary enhancements to meet desired enterprise security objectives.

The ESA is an ongoing set of activities, base-lined annually. These activities are directed by both internal and external drivers as shown in Figure 14, on the following page. Internal drivers include the NRC Mission, Strategic Plan, Management directives, and Information Technology and Information Management Roadmap that guides the Agency's most important business needs. External drivers include Federal Enterprise Architecture (EA), NIST GAO, and industry best practices. Each annual iteration will align with the PMM phases for consistent management. With each iteration, the ESA will be revised and measured against the GAO EA maturity levels. Throughout this process we will review the ESA for compliance to SOW objectives to include 2010 FISMA reporting requirements, HSPD-12, IPv6 requirements, and NRC guidance. We will also assess maturity with SANS Institute Consensus Audit Guidelines and support separation of duties.

ESA Drivers and Lifecycle

Iterative ESA processes continuously mature the NRC Cyber Security Program to achieve more streamlined operations with less technology and greater PMM efficiencies by systematically collecting operational information, assessing it, and responding to it. The Target ESA and Transition Plan will provide valuable progressive sustainment to the NRC – affecting elements such as policy, processes, standards, and tool use. These changes are made to the NRC Cyber Security Program, and coordinated with other NRC functions to influence mechanisms such as the PMM.

Figure 14. ESA activities follow the PMM and result in continuous maturity on an iterative basis.

These changes will provide greater operational efficiencies for achieving security and compliance. This benefits the NRC Cyber Security Program, System Owners, and PMM practitioners by enabling security and compliance to be achieved more consistently with lower cost and effort.

In addition, SOW activities such as Evaluation of New Technologies, Analysis of Best Practices, and Security Relevant Business Solutions are sometimes performed in response to the Target ESA and transition plan. Any time these activities are performed their results are captured and assessed as part of the continuously evolving Target ESA.

Further, as systems are developed, assessed for ATO, and continuously monitored, important information will be captured and received by the ESA program. This information will be used to maintain the documented "As-is" ESA and assessed to drive the definition of the Target ESA. Examples of the internal and external drivers that will be collected and assessed by the MAR Team for Target ESA definition are included in Figure 14.

We will use proven ESA processes for capturing and holistically assessing this information. This analysis identifies patterns and other data that indicates the best focus areas for maturing the NRC Cyber Security Program. We will focus on:

- **Metrics** – For each operational activity in accordance with defined processes.
- **Lessons learned** – From activities such as system authorization and continuous monitoring.
- **Assessment findings** – Aggregated findings from vulnerability assessments and penetration tests conducted for C&A and continuous monitoring.
- **Waivers** – As requests are made to waive certain standards, these are captured and evaluated to determine if the standard is still relevant or in need of a refresh.
- **Incident Information** – Assessed in the aggregate with focus on incidents that consume the greatest amount of NRC resources or represent a greater impact to the NRC mission.

As the ESA processes matures and data collection becomes more clearly defined, we will assess existing NRC tools and adopt them to automate aspects of the collection and analysis process.

The ESA Drives Operations

Recommendations that are developed improve operational efficiencies while maintaining security and compliance. Recommendations that support the ESA Framework and drive the operations have an appropriate business case and represent a positive ROI and are typically in the form of:

- **Policy enhancements** – Such as enhancements to Management Directives.
- **Strategy, Framework and Plan enhancement** – To include revisions to the RMF or the Business Continuity Plan.
- **Process enhancements** – Opportunities to perform processes more efficiently or appropriately, such as the scanning of multiple systems at one time as part of Cyber Situational Awareness activities.
- **Standards enhancements** – Opportunities to introduce new standards and refresh those that no longer fit well, such as those that are repeatedly waivered.
- **PMM enhancements** – Opportunities to enhance PMM activities and tools in a way that better ensures successful ATO for systems.
- **Tool enhancements** – Opportunities to adopt standard tool configurations and settings for faster and more consistent execution across projects, such as vulnerability scanner settings and reporting details.
- **TRM and IT Catalog Updates** – Opportunities to update the TRM and IT Catalog by eliminating or replacing current options and introducing new ones.
- **Business Solutions** – Opportunities to better meet business needs with specific solutions.

In some cases, recommendations involve changes to capabilities outside the NRC Cyber Security Program, such as an enhancement to the PMM that helps project teams more efficiently build security into an IT systems and increase consistency of controls across systems.

Recommendations will be socialized and prioritized with Security Officers and key stakeholders, and can take two possible paths to implementation:

- **Normal Track** – Recommendations and updates will be incorporated into the Target Architecture and the subsequent Transition Plan as part of the normal ESA Development Process.
- **Fast Track** – Approved recommendations move directly to the appropriate change agents for more immediate action. The changes become part of the revised As-is Architecture and are reflected in the downstream ESA Development Process. This allows the NRC to quickly benefit from more compelling changes without waiting for the next iteration of the Target ESA and Transition Plan.

Recommendations will be expressed in the context of the ESA Framework and evaluated against the ESA Principles. The ESA framework and principles will be developed in collaboration with appropriate NRC organizations, and address topics such as separation of duties and least privilege. The Framework draws on the Federal Segment Security Architecture Methodology and the principles draw on NIST 800-14, Generally Accepted System Security Principles.

ESA Deliverables

Table 6, ESA Deliverables, defines and describes the NRC ESA deliverables in the context of this lifecycle and the actions the MAR Team is responsible for to ensure all ESA deliverables are current and complete. The deliverables complement each other and are managed holistically by the MAR Team ensuring a complete and efficient ESA program for the NRC.

Table 6. ESA Deliverables
ESA Deliverable 1 – Annual Project Plan: Updated annually to re-baseline the plan, incorporating a PMM compliant Integrated Master Schedule while clarifying and tracking scope, time, cost, risks, and quality. This plan further identifies and tracks resources. The Plan is baselined during the PMM Inception phase and provides updates to the COR at least quarterly. This is tracked and managed using the MAR PMOS to ensure uniform reporting and consistent quality management.
ESA Deliverable 2 – Charter and Communications Plan: The development and maintenance of the ESA Charter and Communications Plan is accomplished in collaboration with the COR and the NRC organizations critical to the definition and implementation of the ESA. This includes the ESA objectives which are refreshed annually and articulated as part of communication plan activities.
ESA Deliverable 3 – Annual "As-Is" ESA: The ESA Framework is used to capture, track, and report the Annual "As-is" ESA status. Policies, standards, processes, services, and the TRM are included in this analysis and are reflected in this deliverable. Changes to the NRC's security mechanisms are continuously captured to enable rapid visibility into the current "As-Is" ESA at any point in time. Utilization of other activities, such as continuous monitoring, supports the on-going validation of the current state of the "As-Is" ESA. On an annual basis a complete review and validation of the continuously captured "As-is" ESA information is performed and a compiled revision is published highlighting key changes from the previous year. This occurs during the PMM Elaboration phase.
ESA Deliverable 4 – Annual Target ESA: The Target ESA defines the intended state of NRC's security capabilities up to three years out as a look-ahead projection. It defines the "to-be" state of elements such as NRC policies, standards, processes, services, and the TRM. A full, formal Target ESA publication is produced annually, and continuously evaluates and updates the Target ESA throughout the year. The ESA Framework is used to articulate and report the Target ESA which also allows for easy comparison to the "As-is" ESA. The ESA Charter and ESA Principles drive the Target ESA. In turn, the Target ESA may define changes to the ESA Charter and Principles over time. We capture and assess both internal and external drivers as the Target ESA continuously evolves. Drivers include regulatory requirements, the Strategic Plan, IT Roadmap, TRM and other drivers described in the *ESA Drivers and Lifecycle* section.
ESA Gap and Transition Plan: ESA gaps are identified and a set of strategies are documented and maintained for transitioning NRC's security capabilities from their current state to their target state. The strategies define the incremental steps necessary to address the gaps and achieve the desired target-state. Specific strategies define the NRC organizations, activities, and artifacts necessary to achieve the target, and typically result in one or more individual projects. The collection of projects across all strategies is managed as a holistic portfolio. Where appropriate, each project in the portfolio follows the PMM as a stand-alone project. The collection of strategies is aligned to the ESA framework and address topics such as: • *Enterprise Authentication*, including a transition to HSPD-12 • *Enterprise Infrastructure Security* including a transition to Internet Protocol Version 6 (IPv6). • *Enterprise Logging* including the establishment of an NRC authoritative time-source for providing a single, accurate, and consistent system date and time; as well as a plan for ensuring all appropriate NRC devices use the time source, log an appropriate level of detail, and retain the logs in a consistent manner, and purge the logs at an appropriate time.
ESA Framework: Development of the ESA Framework utilizes the Federal Segment Architecture Model and the latest SANS Consensus Audit Guidelines as the basis for a framework to capture, track, articulate and report ESA maturity. The "As-is" and Target ESA, and the ESA Transition Plan are expressed using this framework for consistency and ease of comparison. The MAR Team initially defines this framework and updates it annually.
ESA Principles: The NRC ESA Principles are defined and annually updated. The documented ESA Principles establish high-level parameters for achieving the ESA objectives. This includes principles such as: • *Securely Enable Business:* The architecture must enable the NRC's mission while protecting it. • *Appropriate Security Levels:* The architecture must ensure security levels applied to resources are commensurate to their value to the organization and sufficient to contain risk to an acceptable level. • *Agility*: The architecture must accommodate varying security needs. • *Interoperability*: The architecture must provide integrated security services to enable the enterprise to conduct safe and secure business electronically. • *Enable Analysis*: The architecture must provide an authoritative system time and date source that enables service-wide root cause analysis.

The ESA Ensures Success

The continuous evolution of the NRC Cyber Security Program provided by the MAR Team's ESA capabilities ensure the NRC will keep pace with evolving technologies, threats, and regulations. It uses the NRC's past maturity and success as a foundation and strategically moves the NRC to the desired state of architecture maturity.

1.A.6.3 Vulnerability Assessments

RFP Section E, pages 5-6, SOW 8.6.3, pages 19-20

We will rely on our extensive NRC Vulnerability Assessment experience to identify any weaknesses, vulnerabilities, and insecure configurations that pertain to infrastructure or the handling of data. Our assessment methods allow for the comprehensive evaluation of all potential vulnerabilities while providing a full mapping back to applicable security controls in order to provide actionable information on both the remediation and mitigation of all vulnerabilities identified. In this manner, the MAR Team identifies risk to the organization and promises insight regarding the significance and priority of vulnerabilities that should be addressed. We understand that all vulnerabilities are not equal and cannot be effectively identified and assessed without the appropriate application of tools and methods. In order to accomplish this, we will start with checklists stored in MAR PMOS as an initial point of reference for testing. These checklists were developed and are constantly revised based on prior assessment activities on NRC systems. We will use five different testing methodologies as described below.

Testing Methodologies

Analysis. Each aspect of a system must be viewed in the context of its role within both the system and the environment that it resides. To that end, our approach to the review of all documentation pertaining to a system ensures that both compliance requirements are met and that continuity with all other system information is attained. As an example, when reviewing specific sections of a SSP the following steps will be executed:

- The contents of a given section are checked for information that satisfies the requirements of the control(s) applicable to that section.
- The responsible personnel for ensuring the control has been satisfied are verified as being appropriate within the context of their assigned duties within the rest of the document.
- The approach to satisfying the applicable control(s) is reviewed to make sure that it is consistent with the approach taken to fulfill complimentary controls within the SSP.
- The approach to satisfying the applicable control(s) is reviewed for accuracy and to make sure that compliance can be validated in a repeatable manner.

Demonstration. Our engineers have conducted extensive information security vulnerability assessments throughout both the federal and commercial environments. This experience allows us to fully understand both the information security controls that may apply to any given system, as well as the recommended technical approaches for implementing those controls. This foundation of knowledge and experience is vital to any information security assessment because it provides the ability to not only understand how a security control has been addressed but also how familiar system personnel are with the implementation of that control. We understand that compliant documentation falls short of effective risk management if the personnel identified within that documentation are not capable of efficiently executing the responsibilities for which they have been assigned.

Interview. From our experience in conducting vulnerability assessments, we have found that conducting the interviews prior to reviewing demonstrations of system and personnel capabilities is key to identifying appropriate personnel for the demonstrations. This approach increases efficiency of the vulnerability assessment process without introducing additional steps. Following a review of the documentation available for a given information system, we will conduct interviews of all personnel identified within that documentation to verify that the system stakeholders are aware of their assigned responsibilities and also knowledgeable on the approach to be taken to satisfy the controls. In this manner, our team will validate the accuracy of the information within the system documentation and also prepare for the demonstration phase of our assessment process.

Inspection. As described above, we will validate all information security controls deemed applicable to a system or environment. This approach is not limited to technology. For example, our engineers understand the difference between a dry-pipe fire suppression system and a wet-pipe fire suppression system and are prepared to communicate with facilities personnel to validate documentation pertaining to these systems. Proper visitor control is very important and we will review documented procedures and also conduct inspections of sign-in logs for controlled areas. Our engineers also fully understand the critical nature of correct media-handling procedures and are prepared to review the physical and environmental controls in place to ensure that NRC information is only accessible to authorized personnel. Our approach to the inspection of applicable security controls is based upon the understanding that everything we do must be measurable and repeatable. This understanding does not allow for anything less than complete validation.

Technical Test. We understand the importance of not only verifying that the systems' configuration(s) are identical to their documented settings, but also validating that those configurations are performing as intended. For this reason, our engineers first review all configuration files and settings on devices, computers and appliances and then conduct comprehensive assessments designed to test the effectiveness of those configurations. For example, if a Windows 7 system's documentation states that it is intended to use only a specific set of TCP protocols for communication with other systems, our engineers will validate this by logging onto that system and running the netstat command with the appropriate command line arguments to verify that only the specified ports and protocols are listed. Our engineers will then conduct a port scan of that system that addresses all 65,535 TCP ports to ensure that the information obtained via both the netstat command and the system documentation are accurate.

The assessment provides a detailed point-in-time security analysis of the key components within the system boundary. By using our in-depth expertise in the security of networking, network devices, operating systems, and key applications, our assessment will detect security vulnerabilities and weaknesses that result from how components are installed, configured, and administered.

Our engineers have comprehensive experience conducting vulnerability assessments in both the federal and commercial markets. They have professional certifications that include, but are not limited to the CISSP, GWAPT, and GCIH accreditations, and they have been recognized as leaders in the field at both information security conferences and federal agency councils. This experience and leadership differentiates the MAR Team as being uniquely qualified to not only conduct every aspect of vulnerability assessments with the utmost professionalism and efficiency, but to speak with authority on industry best practices, emerging threats and mitigation approaches in use across the information security industry. This foundation of knowledge, depth of experience, and proven efficiencies will be evident through the analysis, personnel interview, demonstration, inspection, and technical testing of NRC systems.

1.A.6.4 Source Code Reviews

RFP Section E, pages 5-6, SOW 8.6.4, pages 20-21

- *MAR has supported NRC Source Code Review initiatives since 2010.*
- *MAR team member Chris Young has participated in visits to the SAAS vendor facility to enable NRC to complete the vendor assessment in FY12*

A two-pronged approach is proposed for the review of application source code for vulnerabilities in support of the NRC Cyber Security software assurance effort. We will provide continued support for the assessment of auditing software. This software is intended to identify flaws in source code in order to minimize vulnerabilities and risk to the NRC. Independent verification of applications will be conducted for vulnerabilities during the SDLC. Our Team will continue our support of the CSO in the assessments of offsite Software-As-A-Service (SAAS) vendor facilities to ensure NRC source code being evaluated at the facility is properly protected.

This approach supports current and upcoming NRC requirements. The PMM specifies that risk is addressed throughout the SDLC and provides secure coding practices for development teams. Further, the proposed new Web Application Standard, currently under review by the NRC Standards Working Group (SWG) includes security requirements based on the Open Web Application Security Project Top 10 web application risks for 2010 and prior years and will apply to NRC web applications. The MAR Team led the development of the Web Application Standard.

Providing a method to proactively test the security of applications will enable the NRC to include security as a core component of software development practices. Developers will be able to address security vulnerabilities earlier in the SDLC as software is being created.

The two goals of static source code testing are to proactively identify and provide information to developers which enable them to fix security vulnerabilities early within the SDLC, and to mature CSO's capability to independently assess applications against applicable security requirements. The Team will work with NRC to develop and finalize agency-wide requirements and procedures around static application security testing.

Proactive Developer Verification

The MAR Team will identify, discuss, research, and evaluate current practices and tools (COTS, GOTS, and other) used by NRC's IT system developers to identify application security vulnerabilities that exist as a result of flaws and inadequacies in the source code throughout the different phases of the SDLC. We will build on work performed over the last two years for CSO to identify and evaluate appropriate source code analysis tools to support software assurance.

We provide CSO with reports describing the current practices and tools in use among NRC's IT system developers. The report identifies the practices and tools in use that identify application security vulnerabilities in line with the proposed new Web Application Security Standard and the secure coding practices for development teams described in the PMM. If current practices and tools cannot provide the proactive developer testing capability envisioned by CSO, we will research alternate approaches to include a combination of manual processes and tools.

CSO Verification

We have assisted the NRC in performing security assessments of the static source code analysis SAAS provider to expand the pilot use of the service to allow for greater use in the agency. The MAR Team will continue work to establish formal requirements around the use of the SAAS service to fully implement the use of the service and to establish compensating operational controls in order to reduce residual risk that remains due to the SAAS nature of the solution.

By providing these source code analysis capabilities, the NRC is able to include security throughout the SDLC, to expand the Cyber Security software assurance effort, and to meet goals in the IT/IM Strategic Plan. The source code analysis capabilities will assist the NRC in providing specialized security training for software developers to incorporate security controls during the next fiscal year development phase and to expand security testing in the following fiscal year in accordance with the IT/IM Strategic Plan goals.

- *The MAR Team members have independent facilities and teams dedicated to penetration testing.*
- *MAR Team members have recently attended intelligence community penetration testing boot camp, as well as Core Impact related training.*

1.A.6.5 Penetration Testing

RFP Section E, pages 5-6, SOW 8.6.5, pages 21-22

A critical element in effective enterprise cyber security risk management is the ability to identify potential risks posed by internal and external threats. Penetration testing is one means of identifying these risks – by having skilled security experts use the tools and techniques that malicious parties may attempt to use against NRC networks.

The MAR Team brings a unique capability and focus on penetration testing. Successful penetration testing depends on the expertise and skills of the testers. Our Team includes reach back capability to over 100 highly skilled personnel with proven expertise in penetration testing tools, techniques and methodologies in both the private and public sectors. We also have key partnerships with world class penetration testing products and firms. As examples, we have:

- Industry-recognized pioneers in security testing software and methodologies with pedigrees from elite ethical hacking firms at @stake, Symantec, Neohapsis, and many others.
- Published authors of penetration testing books and articles.
- Recognized speakers at industry conferences including the DHS Software Assurance Forum, GFIRST, $(ISC)^2$ Security Congress, OWASP AppSec, and many more.
- Partnerships with leading penetration testing vendors such as Rapid7 and supporting their professional services teams in conducting penetration testing.
- Contributors to the Metasploit project in developing new and custom exploitation plug-ins.
- Developers of the OpenVAS security testing suite.

Penetration testing is a special class of security testing in which assessors mimic real-world attacks to identify methods for circumventing the security features of an application, system, or network. This often involves launching real attacks with tools and techniques commonly used by attackers. Penetration tests can be executed from various perspectives and focuses including:

- Network penetration test,
- Web application penetration test,
- Social engineering,
- Red team/blue team,
- Wireless penetration test,
- Embedded application assessments.

The goal of penetration testing is to determine:

- The survivability of the system in the face of real-world attack patterns.
- The sophistication/resource levels required for an attacker to successfully penetrate the system.
- Additional controls and countermeasures for protecting against the most likely attack types.
- The NRC's ability to detect attacks and respond accordingly.

While penetration testing may not be appropriate for all systems, applications or networks, the data obtained from rigorous penetration testing is a valuable element in providing a holistic assessment of NRC system security. As an input to the ESA, these test results can be used in the context of security control assessments, vulnerability assessments, system security plans, continuous monitoring results, and other data sets to provide greater cyber security awareness to the NRC.

We will coordinate with the CSO in developing a penetration-testing program to create and maintain a flexible and scalable capability to perform a variety of penetration tests. Pursuant to the RFQ, the MAR Senior Project Manager, Mr. Evans, will request the COR or alternate COR to be present during all active penetration testing.

This penetration-testing program uses best-in-class COTS (Core Impact, Immunity CANVAS, Sensepost Labs BiDiBlah, BackTrack Enterprise) and open-source tools (Metasploit Framework, w3af, Burp Suite, Paros Proxy, nikto, wikto), as well as the latest testing techniques (fuzzing, SOAP/LDAP/Xpath injection, SSL renegotiation attacks). We also bring leading edge research and development in custom tools that have been developed over hundreds of penetration testing engagements. This is vital in maintaining a level of adversarial parity, and to provide the most realistic real-world attack scenarios. The list of tools used by the MAR Team is maintained in a Tools Report, which is approved by the NRC prior to engaging in any testing activity.

"Red Team", or external penetration testing, is performed using the broadest possible attack context. Penetration testing of a single host, application, or network in an isolated manner may not

provide the fullest assessment of the security posture of the system. The system may interconnect with or lie on the same network as a more vulnerable system. While the individual target may prove resilient to external attack, it may be less resilient to side-band attacks from more vulnerable proximal systems. The testing focus for Red Team testing will vary depending on the nature of the system to be tested but will include brute-force attacks, buffer overflows, injection, and protocol manipulation. Denial-of-service tolerance will also be measured as requested.

Application penetration testing is more readily performed in an isolated context since the goal of this testing is to determine the survivability of a particular service or interface. This testing will primarily focus on the software engineering and implementation aspects of the application such as input validation, identification and authorization, access control, bounds checking, and other common vulnerability sources.

The testing focus for "Blue Team", or internal penetration testing, is to assess the resilience of internal controls to attacks signifying a successful external penetration or the activities of a malicious user or agent on the internal network. Key testing areas will include privilege escalation, privilege hijacking, credential capture, broad access control testing, and other inference-based attacks made possible by positioning within the network and by access to internal directory and file services (e.g., LDAP, Active Directory, and NFS). Blue Team penetration testing may also include elements of social engineering where appropriate.

Social engineering covers a range of activities whereby an attacker attempts to test the human element of security and can reveal weaknesses in user awareness or behavior, such as failing to follow standard security procedures or performing proper authentication. Social engineering attacks fall into two categories: human-based attacks that use person-to-person contact and technology-based attacks, where users become the unwitting initiators of a code-based attack.

At the direction of CSO, we will engage in social engineering attempts against NRC staff/contractors, using any or all of the recognized social engineering attack types as shown in Figure 16.

Figure 15. Examples of Social Engineering Attacks.

In preparing for penetration testing, our Team will sign any appropriate Non-Disclosure Agreements (NDA) and will develop a project plan and execute the plan in accordance with the following steps/phases:

- **Phase 1 – Information Gathering:** For each penetration testing engagement we will coordinate with CSO to identify the targets, means, methods, duration, and other pertinent descriptors for the effort, including identification of external (Red Team) and internal (Blue Team) elements, application-level testing requirements, and level of social engineering requirements, if any.
- **Phase 2 – Testing Tools:** Appropriate tools will be selected for the engagement from the Master Tool List and incorporated into a Tools Report for submission to the COR for review and approval. Upon approval and prior to loading the tools, the testing team will update all penetration testing devices with the latest security patches, updates, and plug-ins. At the completion of the testing these devices will be wiped clean and notification will be provided to the COR.
- **Phase 3 – Test Plan:** A detailed penetration-testing plan will be developed and submitted for COR approval. The test plan will include:
  - Testing personnel,
  - Tool list,
  - Types of tests,
  - Go/No Go criteria,

  - Target list/User community,
  - Schedule,
  - Rules of Engagement,
  - Start/stop dates and times,
  - Emergency Points of Contact,
  - Contingency List,
  - Anticipated results/Testing breakpoints,
  - For social engineering attacks, this may include additional coordination, waivers and/or other protections to mitigate adverse target reactions,
  - Audit Risk determination.

- **Phase 4 – Testing:** Penetration Testing will be performed at an NRC-approved location and is subject to observation by a CSO-designated NRC staff member. All raw scanning and testing information will be captured during testing activities then stored in a secure manner. The MAR Team will use a suitable, CSO-approved secure archive capability for the storage and sharing of this information with designated personnel. During testing all electronic activities will be logged. Testers will maintain written logs containing observations and findings. Successful exploits or discovered vulnerabilities will be recorded using screenshots. Periodic reports will be made available to approved NRC personnel. Where specified in the rules of engagement, testing breakpoints (i.e. access to a specific file/database/system or root access) will prompt immediate notification.
- **Phase 5 – Test Result Report:** The Test Result Report will present a review of the Test Plan and a timeline of testing activity. This will include how the test was performed, the type of test, and the host/users and their associated organizations that were tested. Successful exploitations will be described in detail with provided screenshots and other artifacts to allow verification and reproduction of the issue. Recommendations will be provided for each finding. The Test Result Report will provide an overall risk rating and recommended guidance on how to mitigate the discovered weaknesses and will outline additional necessary security controls.
- **Phase 6 – Cleanup:** We propose using Virtual Machine (VM) technology to provide clean workspaces for each penetration testing effort. At the conclusion of each test relevant data is extracted from the VM, and the VM is destroyed, preventing information leakage. The VM destruction is verified by the NRC representative observing the testing and will be provided in writing by MAR to the NRC. This is superior to more typical computer images as it avoids issues with changing hardware and drivers. In addition, it scales well to larger test efforts that may require more penetration test workstations.

1.A.6.6 Security Impact Assessments (SIA)

RFP Section E, pages 5-6, SOW 8.6.6, page 22

MAR and CSO worked together in refining the SIA process.

Throughout the ATO lifecycle of a system there may be a need to make changes to the system that may impact the security posture as a whole. These activities are an integral part of configuration management, control, and continuous monitoring which are required by the FISMA and OMB. The NRC has put in place a process to perform Security Impact Assessments, now call SIA, in order to address such situations. The SIA process can be categorized as follows:

- Boundary or data sensitivity changes.
- System interconnection or user base changes.
- New or upgraded software, hardware, or technology.
- Security controls, ports, protocols, or services.
- Physical environment or location changes.

The MAR Team Project Manager will assign an analyst that is familiar with the system requiring an SIA. This will expedite the process by reducing any learning curve and provide for a level of consistency when completing information in the SIA. Using the latest approved version of the SIA form found on the CSO website the analyst will meet with the System Owner to collect the information necessary to complete the form. Our analyst will support the System Owner in following the process outlined on the CSO website in order to submit a fully completed the SIA

form to CSO. Upon receipt of the guidance memo from CSO, we will work with the System Owner to interpret the guidance and assist with the corresponding activities that CSO requires for approval of the system change. These activities may include:

- Updating of Authorization documents (including Security Categorization, SSP, SRA, and other associated artifacts).
- Developing of a component specific vulnerability assessment report that describes the technical risks associated with the change to the components.
- Conducting a tailored ST&E for assessing the changes made to the system.
- Assessing the overall impact of this change to the NRC information system or infrastructure.

Our analysts will work with the System Owner to address the direction provided by CSO, which may include the updating of authorization artifacts and supporting documents. Throughout the SIA process the QA Team will provide oversight and at the completion of the process, will conduct a lessons learned debrief. Information from the lessons learned debriefs will be entered into PMOS or the appropriate NRC repositories.

1.A.7 Policy, Standards, and Training

RFP Section E, pages 5-6, SOW 8.7, page 21

As a member of the NRC Standards Working Group since its inception, MAR has and will continue to apply our experience, technical skills, and best practices to ensure federally mandated policy, standards, and training objectives are consistently achieved.

The MAR Team will provide the NRC support for the creation and maintenance of NRC Cyber Security policy and supporting documentation as well as offering community awareness, training, regular communications, and potentially a conference to increase knowledge, understanding and recognition of Cyber Security across the agency.

We will support the NRC efforts to create, revise, review, and gain concurrence of Cyber Security policy, processes, procedures, templates, guidance, and security relevant business solutions. In addition to our support for the creation or revision of these documents, we also develop, maintain, and deliver Cyber Security awareness and role-based training courses. Upon the request of the COR, we will coordinate and run an annual Cyber Security conference. The NRC will benefit by increasing awareness, knowledge and understanding of Cyber Security throughout the agency. We will also support Cyber Security community communications through the development of a monthly security newsletter and establishment and maintenance of the CSO web site.

These efforts enable the NRC to continue to expand and mature the supporting Cyber Security documents including processes, procedures, templates, guidance, and security relevant business solutions. Our support in these areas also provides awareness of the current state of the NRC Cyber Security Program including changes to requirements, risks, and threats that must be considered.

1.A.7.1 Cyber Security Policy

RFP Section E, pages 5-6, SOW 8.7.1, page 22

The MAR Team supports on-going revisions and maintenance of Management Directive and Handbook (MD) 12.5 NRC Cyber Security Program. MD 12.5 defines the NRC Cyber Security Program, lays out the framework for the Program, and provides requirements for securing information technology systems and devices. We will assist in finalizing and keeping MD 12.5 up-to-date given the role of MD 12.5 in specifying the objectives for the Cyber Security Program. If CSO deems that changes are needed, we will perform the necessary research, propose revisions, and work with

Beginning in 2009, the MAR Team provided support to revise MD 12.5 Directive and Handbook:

- *Performed research and provided proposed new content.*
- *Obtained, reviewed, discussed, and responded to CSO and Program Office feedback.*

CSO and program offices to obtain feedback and gain concurrence for the revisions. This acts as an important driver for the strategic planning and operations of the CSO. Further, MD 12.5 lays out the responsibilities of program offices and individual roles within the NRC. MD 12.5 provides critical guidance and directly supports the work of the CSO as well as the work performed by other Program Offices as part of the overaching Cyber Security Program.

Any revisions to MD 12.5 will be aligned with the 12 primary areas of the policy framework provided by the ISO 27002:2005(E), "Code of Practice for Information Security Management."

1. Access Control,
2. Asset Management,
3. Business Continuity,
4. Communications and Operations Management,
5. Compliance,
6. Human Resource Security,
7. Incident Management,
8. Information Systems Acquisition, Development, and Maintenance,
9. Organization,
10. Physical and Environmental security,
11. Risk Assessment, and
12. Security Policy.

We understand that changes to any of these 12 areas and the associated security considerations within each, has the potential to impact the overall Cyber Security Program and to the Program Offices and systems. Our knowledge and experience with program requirements and systems across the NRC enterprise enhance our ability to improve communication and awareness, proactively facilitating compliance with MD 12.5. Our participation in other activities, such as role- based training, provide a unique opportunity for us to assess and determine revisions to the training curriculum as MD 12.5 evolves. Through the MAR Team's experience supporting the MD 12.5 revision requirements over the past three years we are well equipped to continue this support to help mature the Cyber Security Program through timely and proactive policy updates and user community communications.

1.A.7.2 Processes, Procedures, Templates, Checklists, Standards, and Guidance

RFP Section E, pages 5-6, SOW 8.7.2, pages 25-26

MAR will continue to provide support to the CSO in strategic planning, facilitating inter-office collaboration, and developing procedures, standards, and guidance that address federally and NRC mandated, and standard industry best practices governing computer security requirements.

Our Team will draw upon our experience in support of the NRC across the organization to:

- *Support the maintenance of the strategic Standards Roadmap;*
- *Promote collaboration between the NRC's Standards Working Group member offices;*
- *Facilitate the success of the Standards Roadmap by developing and maintaining policies, procedures, and standards relevant to the NRC Mission and in alignment with Federal and industry security standards.*

The NRC's computing environment is comprised of a wide variety of technologies to enable the NRC to perform its mission. The NRC is obligated under FISMA legislation to make certain that federal computing system configurations are compliant with established acceptable configuration requirements. In order to accomplish this, the NRC CSO has continual requirements for policies, procedures, standards, and guidance that comprise the security governance for the agency overall.

We will support NRC Cyber Security Program's requirements by providing documentation development, maintenance, and implementation that focuses on the security controls outlined by NIST SP 800-53.

- Access Control
- Security Awareness and Training
- Auditing and Accountability
- Maintenance
- Media Protection
- Physical and Environmental Protection

- Certification, Accreditation, and Security Assessments
- Configuration Management
- Contingency Planning
- Identification and Authentication
- Incident Response
- Planning
- Personnel Security
- Risk Assessment
- System Services and Acquisition
- System and Communications Protection
- System and Information Integrity

Because of the dynamic nature of potential threats, vulnerabilities, and related regulatory compliance requirements, Cyber Security is a constantly evolving environment. Our approach to ensure compliance and provide up-to-date security governance documentation involves a continuous monitoring and review process for the creation and maintenance of standards as well as other formal documents including policies, procedures, and guidance as systems, technologies and operational needs change.

This approach includes an annual review and revision of all policies, procedures, standards, and guidance upon request by the NRC's CSO and Standards Working Group (SWG). To support the CSO and SWG, our Team of analysts will examine each document's applicability to the current and future planned state of the NRC's computing environment. Based on these periodic reviews we will work with CSO and the SWG to identify and revise specific policies, procedures, standards, and guidance. We will also conduct annual reviews of revisions made to external checklists that are specified within NRC standards to identify changes, and potential impacts to the NRC. We will communicate summaries of the changes to the CSO and SWG.

The development and revision of the policies, procedures, standards, and guidance considers the following:

- FIPS 199 sensitivities (low, moderate, high) for confidentiality, integrity, and availability.
- Sensitive Unclassified Non-Safeguards Information (SUNSI)
- Safeguards Information (SGI)
- Classified Information
- Different types of information that the NRC must protect
- The ESA Target Architecture and Transition Plan

Figure 16. Security Configuration Standard Lifecycle.

Security standards will be developed and maintained in accordance with the CSO's Process for Development, Establishment, and Maintenance of NRC IT Security Standards. This process, encompassing a nine-phase NRC security standard lifecycle depicted in Figure 16 and described in Table 7, will be followed. For each Phase of the process described, we provide a summary of the action and the work supported and/or accomplished by the MAR Team resources.

Table 7. NRC CSO Security Standard Lifecycle

Phase	Description
1 Configuration Standard Requirement	A requirement for a NRC security standard is identified. We coordinate with the CSO and/or the SWG to identify a configuration standard ("external checklist") to use as the basis for the NRC security standard.

Table 7. NRC CSO Security Standard Lifecycle	
Phase	**Description**
2 Create NRC Configuration Standard	We work with the CSO and/or the SWG to create an initial draft of the security standard using the security standard template. Consultation, as required, is conducted with relevant system ISSOs and SMEs (e.g., contacts in Infrastructure and Computer Operations Division (ICOD), Business Process Improvement and Applications Division (BPIAD), and Nuclear Security and Incident Response (NSIR) as the standard is developed. Feedback from system ISSOs and SMEss is considered and incorporated into the draft as applicable. The NRC's SWG reviews the draft and provides comments and feedback. The changes are incorporated and the draft security standard is approved by the SWG for release.
3 ISSO Forum/ Stakeholder Review	The SWG provides the proposed security standard to OIS for concurrence and provides an informational copy to the ISSO Forum for the purpose of validating applicability and reasonableness. Feedback will be submitted to the SWG.
4 CSO Incorporates Changes	We support the CSO and/or the SWG to review all suggested changes to determine if conflicting recommendations were introduced during the formal review process in Phase 3 and to update the security standard.
5 DAA Approval and CSO Release of Configuration Standard	The SWG and the DAA approve the security standard. The SWG and CSO release and publish the security standard. ISSOs and System Owners are responsible for ensuring that systems comply with the standard.
6 Oversight and Compliance	The NRC effective security standard is used during compliance testing. When tests indicate that an NRC information system does not comply with the standard, a weakness will be added to the system's POA&M to track remediation of the condition.
7 Continuous Monitoring	The security standard is used during the continuous monitoring process to ensure that systems remain configured pursuant to the requirements of the standard.
8 Annual Review/Updates	We coordinate with the CSO and/or the SWG to review each security standard (and the supporting external checklist) at least annually and update the standard as needed related to changes in the threat environment, changes to the external checklist, and new or emerging requirements (such as the release of a version of an operating system). Updates to external checklists do not necessarily mandate an update to the corresponding security standard unless significant changes are required.
9 Retirement	When standards are no longer applicable to NRC's security protection and compliance, the security standard is retired.

We understand the rigorous nature involved in the process of preparing for and obtaining final CSO and SWG approval of policies, procedures, standards and guidance. Through our Team's extensive experience in obtaining and responding to stakeholder feedback, we have successfully worked to obtain CSO and SWG approvals. This emphasis on obtaining feedback and working with stakeholders is exemplified by the recent finalization of Organization Defined Values Standard, as well as the ongoing finalization of the Management Directive 12.5, Web Application Standard, and VMware Standard.

Our structured approach builds on the formation and accomplishments of the SWG and collaboration with NRC program and support offices to develop and maintain the currency of policies, procedures, standards, and guidance. Significant benefits to NRC include:

- Improving clarity of security requirements based on technologies within the NRC.
- Integrating feedback from non-CSO stakeholders to reduce pushback on new and revised requirements.

- Improving alignment of standards and specific security requirements to the technologies specified within the NRC TRM and IT Roadmap.

We have the knowledge and understanding required to effectively navigate the CSO and SWG approval process. The MAR Team has worked closely with the NRC to support the creation, revision, and review of security governance documentation and have supported the continuous improvement of the SWG process and products.

1.A.7.3 Security Relevant Business Solutions

RFP Section E, pages 5-6, SOW 8.7.3, page 26

Our Team has the expertise and capability to research and prepare technical electronic business solutions for new or modified NRC business solutions while addressing security within the NRC business processes. These may include solutions implemented for efficiencies or new initiatives such as cloud computing, mobile devices, and the security required to implement these solutions.

We have the necessary understanding of each NRC system, the user community it supports, the business function it provides, and the impact it has on the office and the agency. For example, MAR Team member KCG's FedRamp 3PAO accreditation brings a cloud computing assessment capability to our Team, and Team member CACI is working on developing applications for tablet devices. We also have the ability to assess the relevancy of proposed solutions and the affects the solutions will have on efficient processing, as well as on security. We will work with CSO to document new solutions within the NRC Cyber Security Program following established processes for the development of standards, processes, procedures, templates, checklists, and associated training needs.

1.A.7.4 Cyber Security Awareness Program

RFP Section E, pages 5-6, SOW 8.7.4, pages 26-27

The MAR Team has and will continue to develop, maintain, and update Cyber Security awareness courses to supplement the current NRC Security Awareness Program including the use of electronic training methods to ensure that federally mandated and NRC defined cyber security requirements are satisfied.

These courses use current technologies such as those used in the current security awareness training that will supplement the current Federal Information Security Line of Business (LOB) and operate within the NRC Learning Management System (LMS). All courses are Sharable Content Object Reference Model (SCORM) compliant.

There are a variety of sources of material on security awareness that is incorporated into our awareness program. The material may address a specific issue, or in some cases, describe how to develop an entire awareness program, session, or campaign. Sources of relevant material include:

- E-mail advisories issued by industry-hosted news groups, academic institutions, or the organization's IT security office.
- Professional organizations and vendors.
- Online IT security daily news websites.
- Periodicals.
- Conferences, seminars, and courses.

Awareness material is developed using one theme at a time or is created by combining a number of themes or messages into a presentation. For example, a poster or a slogan on an awareness tool should contain one theme, while an instructor-led session or web-based presentation may contain numerous themes. Regardless of the approach taken the amount of information should not overwhelm the audience.

Formal evaluation and feedback mechanisms are important components of any security awareness, training, and education program. Continuous improvement of the course materials and educational programs are facilitated when there is a strong comprehension of how the existing program materials and methods are working. In addition, the feedback mechanism must be designed to address objectives initially established for the program. Once the baseline requirements have been solidified, a feedback strategy can be designed and implemented.

If requested, our Team will assist the CSO through evaluation of the effectiveness of security awareness training. As an example, we helped CSO establish a capability to measure the effectiveness of security awareness training among all NRC personnel. Due in part to the findings of an OIG report on Social Engineering (OIG-10-A-11), our Team worked with CSO to use the PhishMe service to measure the effectiveness of security awareness training aimed at educating users on the dangers of phishing. We completed and presented the findings of security awareness testing which tested staff across all NRC offices. The initial phases were successful and highlighted that further education and testing of personnel was necessary to understand the exposure of the problem.

1.A.7.4.1 Course Descriptions

SOW 8.7.4.1, page 27

Course descriptions will include NRC SGI content such as user authentication methods, end user responsibilities, electronic media, electronic handling access and storage, e-mail, use of mobile devices, malicious actor techniques including social engineering, and social networking security considerations. We will also integrate federally provided general user awareness content. As new topics related to SGI or other general cyber security awareness is identified by CSO or other sources, we will coordinate with CSO PSTT to appropriately modify, enhance, and incorporate new information into the existing cyber security awareness materials.

- *MAR developed five highly successful Role-Based Training Courses for the NRC.*
- *YTD 2012 MAR has delivered eight Role-Based courses under the CISSS contract.*
- *MAR has 15 dedicated laptops available for NRC lab-based training courses.*

1.A.7.5 Cyber Security Role-based Training Program

RFP Section E, pages 5-6, SOW 8.7.5, page 27

In order to comply with FISMA, the MAR Team will continue to provide Cyber Security role-based training to NRC staff and contractors with significant security responsibilities. We will continue to develop and deliver role-based training courses that address all FISMA requirements and ensure that all course materials are applicable and current, these courses include:

- Role-based Training for ISSOs
- Role-based Training for System Administrators of Windows-Based Systems
- Role-based Training for System Administrators of Linux/Unix-Based Systems
- Role-based Training for Senior IT Managers and System Owners
- Role-based Training for the DAA
- Role-based Training for Senior Level Managers and Executives

In addition, these courses are developed in accordance with the most recent version of the NRC IT Role-Based Training Plan to provide the agency's IT security workforce a common understanding of the concepts, principles, and applications of IT security that enhance the confidentiality, integrity, and availability of NRC's information systems and IT resources.

In recent years, the MAR Team designed and built a series of role-based, instructor-led training sessions that covered the topic areas listed above (with the exception of Role-based Training for System Administrators of Linux/Unix-Based Systems which is currently in development and

scheduled for delivery in FY2013) and were well received by NRC course participants. Figure 17 provides the high-level work flow in developing and refining the role-based training courses.

Figure 17. NRC and MAR Collaborative Course Development and Delivery Process.

We will continue to engage the services of industry leading experts who specialize in security topics and tools relevant to the NRC to make sure our courses remain current and of value. For example, we elected to use course development methods designed by Dale Carnegie to maximize the learning experience of each participant. This significantly contributed to the success of NRC role-based training courses because it placed emphasis on curriculum that was closely aligned with NRC requirements. In addition, the increased value of having specially trained instructors capable of facilitating complex discussions in both small and large group settings, and the importance of designing a dynamic learning experience that challenges course participants while building confidence in their respective roles and responsibilities was demonstrated. At the conclusion of these courses, participants commented that the hands-on team building exercises that resulted from this approach proved to be demanding, instructional, and entertaining at the same time. Another observation was that these training sessions promoted the establishment of stronger peer networks between security and IT practitioners at the NRC.

Role-based Training for ISSOs

The MAR Team will continue to develop, update and deliver the system and office ISSO course which, at a minimum, will cover the following topics:

- ISSO role in relation to other NRC roles and positions
- Information technology initiatives
- ISSO roles and responsibilities
- Role separation
- Procurement
- Threats
- Vulnerabilities
- Risk management
- Operational, management, and technical security controls
- Planning
- Site/system security plans
- Authorization to Operate
- Continuous monitoring
- Incident reporting
- Continuity of operations

The ISSO role is a trusted position within the agency with special access to and authority over NRC systems. As the principal point of contact for all IT security aspects of an NRC IT system, the ISSO has nearly 40 defined responsibilities. Considered the flagship of role-based training at the NRC, the ISSO course was developed to take full advantage of Dale Carnegie training methods, and affords participants a dynamic learning environment. In part, this is due to the value that CSO staff provides as course participants engage in the review of a variety of programmatic, technical, and interpersonal skills and abilities required of system and office ISSOs, that are necessary to become proficient in such a multi-disciplinary role. Course participants learn about the effective use of NRC organizational risk management practices and techniques, participate in scenario-based role playing exercises (e.g., mitigation of threats and vulnerabilities), learn innovative ways of committing complex learning objectives to memory, and work in team building exercises (e.g., the infamous ISSO Mo' Blues or poetic rendition of security practices set to the Twilight series musical theme). Participants often have remarked that they are pleased with the

course content and the amount of information they were able to retain. They also developed an appreciation of both the importance and demands of the ISSO role.

Role-based Training for System Administrators of Windows and Linux/Unix-Based Systems

The MAR Team will continue to develop and deliver a Windows System Administrators course and Linux/Unix System Administrators course which, at a minimum, will cover the following topics:

- Security configuration guidelines
- NRC policies and procedures
- Authorization to Operate
- Vulnerabilities
- Threats
- Auditing
- Continuous Monitoring
- Incident response

A portion of this class is devoted to hands-on exercises and technical labs that will guide participants in implementing current security configuration requirements for servers and workstations running Microsoft Windows and Linux/Unix. Under the direction of CSO, and building from the ISSO course, we established and commenced training of a Windows System Administrator Course in 2011. Updates to existing courses, and new course development, will focus on security considerations in each phase of a system's lifecycle, and the roles that individuals throughout the organization have in ensuring security is planned, designed, integrated, deployed, and maintained. This approach will include an in-depth review of the roles and responsibilities of system administrators in securing IT systems through implementation of NRC security requirements, adherence to security policies and procedures, awareness of any new requirements communicated by the CSO, and use of security best practices for Windows and Linux/Unix-based systems. For the hands-on technical lab portion of this course, we will provide the necessary lab equipment, setup the gear to accommodate the needs and learning objectives associated with each lab, and support course participants as they navigate the lab exercises. For the benefit of the NRC, future curriculum will be developed in a way to allow for the delivery of either separate courses for each topic area or an integrated Windows and Linux/Unix Administrators' course.

Role-based Training for Senior IT Managers and System Owners

The MAR Team will develop and deliver the Senior IT Managers and Systems Owners course which, at a minimum, will cover the following topics:

- Federal and NRC policies, guidance, regulations and requirements
- NRC FISMA results
- Office of Inspector General (OIG) audits and other NRC auditing or inspection reports
- Planning
- Procurement
- Security in the life-cycle
- Role separation
- Risk management
- System security plans
- Vulnerabilities
- Threats
- Security Controls
- Authorization to operate
- Continuous monitoring

System Owners are agency officials with inherent U.S. government authority for the overall procurement, development, integration, modification, or operation and maintenance of an information system. At the NRC this includes Office Directors, Division Directors within the Office of Information Services, and Regional Administrators. Senior IT Managers at the NRC are responsible for ensuring systems or services meet all agency Cyber Security Program requirements. Examples include regional directors, branch chiefs, team leaders, project managers, management analysts, mechanical engineers, inspectors, health physicists, and technical editors. As a result, the current NRC Senior IT Manager and System Owner course focuses on the establishment of a solid understanding of threats to federal information systems (e.g., Advanced Persistent Threat) and the programmatic means established by the NRC Cyber

Security Program for protection against cyber-based threats. The course is a blending of the more technical, in-depth curriculum of the ISSO and system administrator courses together with the executive security training. Updates and revisions to the Senior IT Manager and System Owner course will address changes within the NRC Cyber Security Program, as well as any feedback received from participants, and the evolution of cyber threats to IT resources deployed throughout the NRC operational environment.

Role-based Training for the Designated Approving Authority (DAA)

We will also develop and deliver a role-based training course for individuals with DAA responsibilities that contain information describing the role and responsibilities for all levels of systems. The course topics are based on relevant NRC considerations and are designed at a high level to help senior level managers and executives evaluate the components of an IT security program. Individuals training for the DAA will focus on the fundamental security concepts necessary to weigh organizational and system-level risks inherent to IT systems for potential impacts to the agency's mission and/or business operations.

Role-based Training for Senior Level Managers and Executives

The MAR Team will develop and deliver a role-based training course for Senior Level Managers and Executives which, at a minimum, will cover the following topics:

- Federal and NRC policies, guidance, regulations and requirements
- NRC FISMA results
- Office of Inspector General (OIG) audits and other NRC auditing or inspection reports
- Overview of the Authorization
- Role separation
- Risk management
- Vulnerabilities
- Threats
- Security Controls
- Authorization to operate

This course will include relevant NRC examples and situations designed to help senior level managers and executives evaluate the components of an IT security program related to NRC business functions and the specific IT requirements. The Senior Level Managers and Executive Course also provide the tools and threat awareness needed to enhance decision making capabilities. This includes knowledge of existing laws and regulations, the NRC's Cyber Security Program, and organization risk management. The training seeks to aid in understanding Federal government and NRC-specific laws, regulations, polices, guidelines, standards, and procedures mandating requirements for the management and protection of IT resources and data. The developed training will continue to foster knowledge of IT to ensure that adequate provisions are in place to protect NRC information that is collected, processed, transmitted, stored, or disseminated within IT systems. This includes heightened awareness of ongoing processes associated with the assessment of risk to IT resources and information, and the determination if adequate security for a system is in place and is being maintained to an acceptable level of risk.

1.A.7.6 Cyber Security Conference

RFP Section E, pages 5-6, SOW 8.7.6, page 30

Upon request of the COR, the MAR Team will provide planning and implementation support for an annual Cyber Security conference for NRC staff and contractors. This conference will provide in-depth coverage of IT security awareness and role-based Cyber Security information. It will be planned for one to three days in duration, and will consist of a multi-track schedule of panels, workshops, and breakout sessions.

A multi-track approach allows the NRC to provide relevant material for all levels of cyber security knowledge and requirements:

- General users will have the opportunity to learn about the goals and intent of cyber security, gain a general awareness from informational sessions, and participate in presentations regarding roles and responsibilities within the NRC Cyber Security Program.
- Cyber Security implementers, such as ISSOs, administrators, developers or other personnel responsible for IT support, design and implementation of NRC systems will be able to attend presentations about advanced technical topics in cyber security.
- NRC Managers and Executives will be provided topics and sessions to highlight the role of IT security from a management perspective, as well as the role of cyber security issues in the planning, budgeting, management, and systems lifecycle of NRC systems.

Conference design may contain a mixture of both informational sessions and role-based training. This approach can combine specific training sessions tailored to the NRC role of the individual, augmented with additional informational or hands-on sessions that provide coverage in areas of interest to the individual or of importance to the NRC.

The MAR Team will assist the COR in developing an initial plan for the conference by addressing the overall goals of the conference, the presentation tracks, and special topics. Conference scheduling, resource requirements, potential topics, qualification requirements for presenters and instructors, and identification of potential presenters and instructors will be planning topics for discussion. As potential areas of interest or presentation topics are identified, we will provide SMEs to assist in the formulation of presentation tracks, session topics, and other relevant information to align the conference material with overall NRC objectives for the conference.

Following review and approval of the conference plan we will develop appropriate workshop material, hands-on training or exercises, or other conference material that is specific to internal NRC cyber security topics. This training will be developed in coordination with PST so that all material is highly relevant to NRC operations, policies, and procedures. The intent of material development is to ensure that the knowledge base provided to conference and session attendees is consistent with internal NRC policy. As a top-level goal, the conference experience will hopefully result in attendees becoming more experienced and aligned with NRC cyber security standards and practices.

We will also offer role-based training materials that use teaching techniques used in previous NRC and other courses, many of which are recognized by the Dale Carnegie Institute, including:

- Memory Stacking
- Scenario-based exercises
- Team-building Exercises
- "Train the Trainer"
- Hands-on technical demonstrations and exercises
- 3D animation presentations

Role-based training will include technical hands-on exercises such as those developed for the role-based System Administrator course which has been well tested through several successful sessions. Other existing role-based and other cyber security training program material will be used where possible, as well as information from NRC, CSO and other publications, standards, guidance, and procedures. It will be important that information and training presented during the Cyber Security conference maintains the maximum relevancy to NRC mission, job functions, personnel, roles and responsibilities, and allows attendees to integrate lessons learned into daily operations. Material may also be developed by invited experts in cyber security topics. Through our existing relationships, we have the ability to engage some of the cyber security industry leaders as listed below to provide meaningful and relevant presentations:

- Dr. Ron Ross, NIST
- Stephen Northcutt, SANS Institute
- Dr. Eric Cole, SANS Institute

- Dr. Sandor Boyson, University of Maryland
- Ralph Langner, Author "Robust Control Systems Networks: How to Achieve Reliable Control after Stuxnet"
- Mark Weatherford, DHS

Presenters will also include key NRC Cyber Security decision-makers and thought leaders, such as the Designated Approval Authority (DAA), internal SMEs, and ILTAB personnel. The MAR Team has identified a number excellent internal NRC resources in the realm of Cyber Security that will provide institutional context and depth to the Cyber Security conference.

Topics may include Advanced Persistent Threat (APT), cyber security trends, critical infrastructure protection, or other topics pertinent to the current threat environment or to the NRC's mission. The MAR Team has successfully developed and presented training courses, briefing materials and demonstrations for NRC staff at all levels, including Role-based ISSO and System Administrator Training, and Advanced Persistent Threat briefing for NRC Management as developed by Dr. Eric Cole of SANS and Michael Shinn of Prometheus Global.

In 2011, the MAR Team assisted the University of Maryland College Park in planning and hosting a cyber security conference on industrial nuclear power. The "Commercial Nuclear Power the Cyber Security Conference" was held on May 4-5, 2011, and was designed to provide a holistic approach to defending against cyber attacks within critical infrastructure and other sensitive U.S. government arenas. Additional details can be found at http://www.oaee.umd.edu/ncsc/. The conference was an unqualified success. Presenters and attendees included: congressional leaders such as U.S. Representative C. A. "Dutch" Ruppersberger, Ranking Member of the House Permanent Select Committee on Intelligence and Member of the House Armed Services Committee; recognized leaders from government and private sector the Cyber Security bodies, including Dr. Ron Ross and Dr. Eric Cole; and organizations such as INPO and the NRC.

1.A.7.6.1 Place of Performance

SOW 8.7.6.1, page 30

The annual the Cyber Security conference location and facilities will be identified at least three months in advance of the conference and will take into account the anticipated number of sessions, session types (speaker, panel, workshop, etc.) and projected attendance. This information is used to determine the space requirements for the conference, and to also allow the NRC CSO to make a determination of the appropriate venues, scheduling, and resources.

1.A.7.6.2 Provided Services

SOW 8.7.6.2, pages 30-31

The MAR Team will provide qualified trainers and presenters in the following areas:

- Operating Systems – VMware, Linux, Solaris 10, Microsoft Windows 7, Microsoft Windows 2008 Servers, Microsoft Windows 2003 Servers, Mac OS.
- Applications - Microsoft Exchange, Microsoft Internet Information Services (IIS), Oracle, Sybase, Citrix, MS SQL Server, MS SharePoint, MS .Net Framework, Apache Web Server, Social Networking software, Blackberry Enterprise Server and Handheld, and IBM Rational Suite.
- Information Assurance - Network Engineering, Network Monitoring, Active Directory, Intrusion Detection Systems (IDS) / Intrusion Prevention Systems (IPS), Firewalls, Virtual Private Networking (VPN), Public Key Infrastructure (PKI), Wireless, Remote Access Systems (RAS), Malware, Spyware, and Penetration Testing.

We have a number of recognized industry experts, many of whom have engaged in successful training and presentations for the NRC. In some of instances, especially the role-based training for ISSOs and System Administrators, SMEs were supported by Dale Carnegie "Train the Trainer"

experience. The trainer's course presentation and delivery were reviewed by Dale Carnegie experts who advised the course presenters in effective presentation, communication and feedback exercises and techniques to further enhance the efficacy of the course content. Other training courses and presentations were given by experienced presenters and trainers, such as Microsoft Certified Trainers (MCT), BlackHat conference presenters, published authors, and SANS-certified trainers. These services will continue as part of our commitment to future NRC training needs.

1.A.7.7 Electronically Communicating Cyber Security Information

RFP Section E, pages 5-6, SOW 8.7.7, page 31

Constant communication related to Cyber Security information and direction is very important to maintaining a high level of awareness to changes in policies, guidance, and the supporting activities to keep the NRC enterprise and infrastructure secure. As described in the previous proposal Sections, the MAR Team is positioned to support user knowledge of security awareness through online and classroom role-based training, and annual Cyber Security conferences where all stakeholders can assemble to learn and exchange ideas. Cyber Security awareness is an on-going daily responsibility. To support the goal of raising and maintaining awareness, we will work with the COR to maintain the existing NRC newsletter FRONTLINE or to develop a new monthly news letter that summarizes changes in policies and requirements. This newsletter will also provide insight as to the current risks and threats that are being seen inside and outside the NRC. Using our understanding of the NRC Program Offices systems and needs, we will place emphasis on how these items impact NRC's ability to deliver their services. We will also assist the CSO in collecting relevant Cyber Security information and in preparing the information for publishing to the NRC CSO website.

As part of our current support under the CISSS program, we have had the opportunity to listen to some of the NRC stakeholders concerns regarding communication about the latest NRC policies, guidance, or requirements. We are familiar with the draft, review, and approval activities that occur within the NRC and within supporting groups such as the Standards Working Groups. We also understand the importance of disseminating information as quickly as possible but only after all approvals are in place. We will work with the NRC to monitor updates to the Cyber Security Program in order to collect and publish via the CSO intranet web site, newsletters, email alerts, and other electronic forms of communication. This information will be reviewed on an annual basis as part of ongoing communication improvements.

While developing and supporting the content in the electronic communication methods we will focus on communicating the ***Why*** of the new standard, policy, or awareness alert. As we have found in conducting the classroom based security awareness training, when the rationale for a process or the consequences of a threat is put in perspective it is better understood and retained by the individual.

With the expanding NRC initiatives for mobile access, Bring Your Own Device (BYOD), and telework, we see a clear benefit in expanding the security awareness program to develop new initiatives in reaching a wider audience through social media and other electronic means. As the NRC workforce continues to expand in its size, mobility, and diversity of work locations, we recommend the expanded use of electronically communication methods to enhance information dissemination across the NRC workforce.

Team member KCG has performed similar work at TSA in producing a cyber security newsletter and as a participant in in-house security seminars. Under a MAR contract with the DOI, we have developed a number of electronic methods to communicate with customers and user community groups. These methods include messages and alerts via email, publishing electronic newsletters, and effective use of their web site to communicate activities and changes. These have been highly successful methods for communicating with existing

stakeholders and customers and reaching out to current and future users. Jane Delgado, a MAR employee, has led this effort in support of DOI, and is also NRC-badged and is a resource available to support the NRC CSPSS program in this task area.

As the Cyber Security Program continues to grow we will review the program on an annual or periodic basis as necessary. We will produce and deliver recommendations to the CSO on more effective methods to communicate with their audience.

Summary

As previously stated our proposal is fully responsive to the CSPSS RFQ and associated SOW. We believe our proposal represents the most cost effective, lowest-risk, and technically superior response to all of the requirements of the RFQ and is of greatest value to the NRC. Furthermore, we believe our combination of highly experienced personnel and team-based management approach will position MAR to effectively support all requirements as stipulated in the RFQ.

1.B MAR, Incorporated's Plan to Comply with FAR Clauses 52.219-6, 52.219-14, and 52.244-2

RFP Section E, pages 5-6, SOW 1.0, pages 1-2

The three Federal Acquisition Regulation (FAR) clauses cited specifically in the solicitation center around the theme of Compliant Subcontract Management. MAR will comply with the requirements related to the following FAR clauses which pertain to Subcontracting.

1. **Satisfaction of Requirements: 52.219-6 Notice of Total Small Business Set-Aside (Nov 2011)**
   MAR certifies it is a small business within the terms of GSA Alliant SB contract and agrees to comply with the requirements in 52.219-6 GS-06F-0641Z.

2. **Satisfaction of Requirements: 52.219-14 Limitations on Subcontracting (Nov 2011)**
   MAR, as a small business, certifies that it will perform at least 50% of the cost of the contract incurred for personnel with its own employees, for the period of the contract (Ref. (g)) Under the GSA ASB Contract, MAR is required to maintain up-to-date records concerning subcontracting costs which includes the submission of a report of subcontracting costs semi-annually (using the contract year) no later than 30 calendar days after each six-month reporting period. On a monthly basis we will internally produce and review a financial report which highlights subcontracting activity and costs incurred and invoiced by our subcontractors. Proactively monitoring subcontracting costs in this way enables us to comply with limitations on subcontracting. As evidence of our commitment to this requirement throughout the life of the CISSS contract order issued by the NRC, MAR has subcontracted approximately 45% of the total work to either subcontractors or consultants. This work was performed under the current MAR GSA IT-70 Schedule GS35F0229K, and the NRC DR3306317 Order. Subcontract management and integration of all team members is very important part of the total Contract and TO requirements.

3. **Satisfaction of Requirements Relating to FAR 52.244-2, Subcontracts (Oct 2010)**
   MAR certifies that it has had a Government approved Purchasing System since 1989. Consent requirements have been waived per this procurement based on the approval of our Purchasing System. This was one of the prerequisite for receiving the GSA ASB contract.

   Subcontracts and Purchasing policies and compliance requirements include the following stages in a procurement within the MAR organization; a) procurement planning and market research; b) prevention of conflicts of interest and procurement misconduct; c) competitive purchasing; d) negotiated procurements; e) cost/price analysis; f) source selection;

g) formation and content; h) foreign purchases and performance; i) procurement management by the MAR project personnel, and procurement administration by the subcontract personnel, inclusive of the subcontract administrator; and j) procurement closeout.

2.0 PERSONNEL QUALIFICATIONS

RFP Section E, pages 5-6

As outlined in Section 1.A.1, our proposed MAR CSPSS Project Organization was developed following SOW Section 8, Task and Deliverables in combination with Attachment D of the RFQ. Within the GSA ASB contract there are 80 labor categories available to support this project. We have carefully selected the applicable ASB labor categories to best meet the requirements of the CSPSS project. Table 8 provides a cross reference for each of our project teams to their corresponding GSA ASB Labor Categories.

Under Attachment D, Overall Contract Responsibilities (CLIN 0001), we have divided the "Financials and Status Reporting" into separate GSA ASB Labor Categories of Financial Analyst and Administration/Clerical (Senior) and placed these positions within the Project Management Team. For "Quality Assurance for Overall Contract only" we created a Quality Assurance Oversight Team and divided the team into GSA ASB Labor Categories Quality Assurance Technical Lead under the GSA ASB Subject Matter Expert (SME) (Senior) labor category and Quality Assurance Support under the Quality Assurance Specialist (Journeyman) labor category.

For the Project Plan and Project Manager Support, we divided the "Project Manager" into Senior Project Manager and Project Manager roles with both being a part of the Project Management Team and mapped to the GSA ASB Project Manager labor category. The Program Manager is a direct mapping to the GSA ASB Program Manager labor category.

For the Technical Teams, which cover all remaining segments of Attachment D and SOW Sections 8.2 through 8.7, we have identified four GSA ASB labor categories of SME, Information Assurance/Security Specialist (IA/SS), Computer Forensic and Intrusion Analyst (CFIA), and Technical Writer (TW) to support the delivery of services for the technical task areas. As noted in Table 8, we have used subcategories for the SME and IA/SS labor categories.

Table 8. MAR Team GSA Alliant Small Business Labor Category Mapping to CSPSS Project Role

Project Role per RFQ	GSA Alliant SB Labor Category
Project Management Team	
Program Manager	Program Manager
Senior Project Manager	Project Manager
Project Manager	Project Manager
Financial Reporting	Financial Analyst
Status Reporting	Administration/Clerical (Senior)
Quality Assurance Oversight Team	
Quality Assurance Technical Lead	Subject Matter Expert (Senior)
Quality Assurance Support	Quality Assurance Specialist (Journeyman)
Technical Teams	
Technical Task Areas Delivery	Subject Matter Expert (Master)
	Subject Matter Expert (Senior)
	Subject Matter Expert (Journeyman)
	Information Assurance/Security Specialist (Master)
	Information Assurance/Security Specialist (Senior)
	Information Assurance/Security Specialist (Journeyman)
	Information Assurance/Security Specialist (Entry Level)
	Computer Forensic and Intrusion Analyst
	Technical Writer

CSPSS Staffing Approach

Based on the RFQ level of effort outlined in Attachment D we have identified a team of approximately 17 key personnel (13 who are NRC badged and three pending badge approval) that represent the leadership and critical SMEs that will oversee all areas of the SOW. We are confident this mix of specific experience and skills will lead the MAR Team's support of activities under the CSPSS project. Table 9 depicts the MAR Team's Key personnel and how each individual will fulfill the SOW areas required under this project. Resumes for key personnel are presented in Section 2.1. Table 10 also includes a list of additional NRC badged personnel that are available to support the CSPSS project.

Table 9. Proposed Key Personnel Labor Categories, Education, and Certification

Employee Name	Labor Category	NRC Badge	Years at NRC	Task Support	Education	Certifications
Bernstein, Michael	Project Manager	(b)(6)	N/A	8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7	Bachelors (In Process)	CISA, CRISC, ITIL V 3.0, MCP, NetWare 4.0
Brody, Bruce	Computer Forensic and Intrusion Analyst		6 months	8.2, 8.6, 8.7	Masters	CAP, Certified Level III Program Manager from DoE, CFCP, CISM, CISSP, ISSPCS
Dickman, Lauren	Administration/ Clerical (Senior)		1	8.1	Bachelors	None
Evans, Thomas	Project Manager		6	8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7	MBA	A+, ITIL V 3.0, Network +, PMP
Kragen, Scott	Subject Matter Expert (Senior)		N/A	8.3, 8.4, 8.6	Bachelors	C)PTS, CEH, CEPT, CISSP, GPEN, GWAPT, OSCP
Pham, Brian	Information Assurance/ Security Specialist (Entry Level)		4	8.2, 8.3, 8.4, 8.6, 8.7	HS Diploma Computer Science Major/ Info Systems Mgmt Major, In Progress	CICP, Hailstorm Professional, ITIL V 3.0
Pollack, Deborah	Quality Assurance Specialist (Journeyman)		2	8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7	HS Diploma	ITIL V 3.0, PMP in progress
Quivey, Rebecca	Financial Analyst		2	8.1	Masters	ITIL V 3.0
Ruf, Brian	Computer Forensic & Intrusion Analyst		N/A	8.2, 8.6, 8.7	Bachelors	CISSP, PMP
Shaw, William	Subject Matter Expert (Master)		2	8.2, 8.6, 8.7	Masters	CAP, CISSP
Shinn, Michael	Subject Matter Expert (Master)		5	8.2, 8.3, 8.4, 8.6, 8.7	Bachelors	FSO, IASO
Simonds, George	Program Manager		6	8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7	MBA, Masters	MSSE Windows 2007 and Windows NT, PMP, Video Polycom Certified Video Conferencing Engineer
Smith, Sandra	Quality Assurance Specialist (Journeyman)		N/A	8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7	Bachelors	None
Tharp, Benjamin	Information Assurance/ Security Specialist (Master)		4	8.2, 8.3, 8.4, 8.6	HS Diploma	CEH, CISSP, IASO, ITIL V 3.0, MCP
Wijetunga, Suneth	Information Assurance/ Security Specialist (Master)		3	8.2, 8.3, 8.4, 8.6, 8.7	Bachelors	CISA, CISM, CISSP, ITIL V 3.0

Table 9. Proposed Key Personnel Labor Categories, Education, and Certification						
Employee Name	Labor Category	NRC Badge	Years at NRC	Task Support	Education	Certifications
Williams, Hank	Subject Matter Expert (Senior)	(b)(6)	4	8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7	MBA, Masters	CISM; CISSP; GLEG; Masters Certificate in Project Management , PMP
Young, Christopher	Information Assurance/ Security Specialist (Entry Level)		2	8.2, 8.3, 8.4, 8.6, 8.7	Bachelors	CompTIA Security +, Intelligence Community Directive 503, MCNPS, MCP, MCPS, MCTS; NSA Blue Team Boot Camp

Additional NRC Badged Resources

Table 10. Additional NRC Badged Resources			
Employee Name	NRC Badge	Education	Certifications
Baker, Blossom	(b)(6)	Masters	CISSP, IAM, IEM, PMP
Burress, Stacy		Masters	ITIL V 3.0
Carey, Maureen		Bachelors	None
Chenoweth, Chris		Masters	Python Certified
Delgado, Jane		MBA	None
Enfinger, Gayle		H.S. Diploma	None
Estrada, Nelson		Masters	CISSP, CompTIA Network+
Evans, Laura		MBA	ISO 9001:2008 Internal Auditor
Figueroa, Nylsa		Masters	CCSA, CCSE, CISA
Finch, Curt		Bachelors	AMA-certified Technical Writer
Green, Joe		Masters	CAS 3.0 ERP SDA
Greenspon, Jeff		Masters	CompTIA Security +, GSEC, ITIL V 3.0
Hackenberg, Dan		Bachelors	None
Haran, James		Bachelors	CISSP
Harren, Robert		Masters	CCNA, CCDA, CISSP, FITSP-M, IASO
Kampas, Walt		MBA	C++
Klages, Linda		H.S. Diploma	ISO 9001:2008 Internal Auditor
Metzger, Kurt		Associates	None
Moore, Jeff		Bachelors	None
Moore, Mike		Associates	A+, ITIL V 3.0, Network +
Norcio, Michael		MBA	None
Payne, Audrey		Associates	ITIL V 3.0, SANS CompTIA Security+
Priester, Casey		Bachelors (in process)	CEH,CISA, CISSP, CompTIA Security +, IAM, IEM, MCSE, SSCP
Riley, Larry		Associates	CISA,CISM, CISSP, CNSP
Sarin, Tarun		Bachelors	None
Shinn, Scott		H.S. Diploma	None
Shorten, Kimberly		H.S. Diploma	None
Spitzberg, Bobbi		Masters	None
Sunukjian, Sam		Bachelors	CMM Internal Assessor, ISO 9001:2008 Internal Auditor
Talkington, Jason		H.S. Diploma	ITIL V 3.0
Williams, LeeAnn		Bachelors	None

2.1 Resumes

2.1.1 Project Management Team

2.1.1.1 Program Manager – George Simonds

Name:	**Simonds, George A. III**	**Company:**	**MAR**
Labor Category:	**Program Manager**	**Employment Status:**	**Employee**
NRC Badge:	(b)(6)	**Country of Citizenship:**	**USA**
Additional Clearance (s):			

Candidates Skills/Experience Relevant to Statement of Work

SOW #	SOW Description	Candidate Qualified
8.1	Project Management	✓
8.2	Special Projects	✓
8.3	System Authorization	✓
8.4	Continuous Monitoring Support	✓
8.5	Data Calls	✓
8.6	Cyber Situational Awareness	✓
8.7	Policy, Standards and Training	✓

Summary of Skills, Experience, and Training/Certifications Relevant to Statement of Work

George Simonds, a PMP certified professional, possesses over 18 years of professional experience in (Information Technology (IT) and Cyber Security. He has several years experience in project management, information assurance, and network and systems engineering, Mr. Simonds serves as a senior manager for specialized projects focusing on Cyber Security regulatory programs and standards development for the Nuclear Regulatory Commission (NRC); organization-wide security policy, standards, and training; full systems lifecycle security management; and bringing complex IT systems into compliance with the Federal Information Security Management Act of 2002 (FISMA), OMB A-130, and the National Institute of Standards and Technology (NIST) Special Publications.

Mr. Simonds current experience exceeds the minimum qualifications of the GSA ASB Program Manager Labor Category. Mr. Simonds role in support of the NRC has evolved over the past six years in correlation with major initiatives undertaken by the agency to significantly improve both internal and regulatory-based Cyber Security programs. This includes award of the NRC's Consolidated Information System Security Services (CISSS) contract in 2006, organization of the NRC Computer Security Office in 2008, associated maturation of the internal Cyber Security program. In 2009 Mr. Simonds supported the establishment of the NRC's Cyber Security regulations under 10 CFR 73.54. He is accustomed to working at all levels of the agency to address programmatic, procedural, and technical challenges across offices, divisions, and branches throughout the agency. Mr. Simonds works closely with executive management for strategic alignment on high profile activities, team leaders and branch chiefs to formulate performance objectives and project plans for associated tasks, and NRC staff to move project activities forward in accordance with executive direction.

Examples of past activities include the timely Certification and Accreditation (C&A) of major NRC systems that contributed heavily to improvement of NRC's overall FISMA scores and assessment of enterprise risks for the betterment of NRC's organizational risk management strategies. He provides briefings to agency executives serving on the IT Business Council for the purpose of discussing approaches for continuous improvement of internal Cyber Security practices. He has provided expert testimony before the Advisory Committee on Reactor Safeguards on the efficacy of NRC's regulatory programs in protecting critical functions at a nuclear power plant (NPP) from cyber-based attacks. He has proposed the formulation of action plans to carry out regional inspections of licensees and COL applicants' Cyber Security programs, and support of program offices' initiatives to evaluate non-NPP licensee facilities for susceptibility to cyber-based attacks.

Name:	Simonds, George A. III	Company:	MAR
Labor Category:	Program Manager	Employment Status:	Employee

Mr. Simonds has led, and continues to lead, multiple teams across a variety of complex, inter-related tasks. His skills in this area are now being leveraged to manage multi-disciplinary teams of Subject Matter Experts (SMEs) across regulatory-focused projects focusing on guidance development, order writing, rulemaking, multi-region inspections, and NRO efforts to document agency business processes and automate regional inspection activities for new plant construction. He also serves as an instructor for NRC's security role-based training, helping design coursework for NRC Executives, System Owners, IT Managers, ISSOs, and System Administrators. In coordination with the University of Maryland, he organized the 2011 Commercial Nuclear Power Cyber Security Conference with guest speakers from Congress, NRC, NIST, DHS, NSA and the university. Mr. Simonds is also involved in the DHS Industrial Control System Joint Working Group (ICSJWG), and recently spoke at the 2012 ICSJWG Spring Conference on topics related to Cyber Security and workforce development challenges across the nation's critical infrastructure sectors.

Mr. Simonds wealth of experience makes him uniquely aware of the NRC mission and business objectives, and he is committed to the ongoing success of its Cyber Security Program. During his tenure as Project Manager on the CISSS contract Mr. Simonds supports of a variety of agency programs resulting in his in-depth knowledge of what it takes to successfully carry out tasks and deliverables as described in Section 8 of the SOW. His positive working relationships with NRC executives, management, staff, and contractors will promote continued improvements in these key areas.

As the Program Manager for Cyber Security Program Support Services (CSPSS) Mr. Simonds will provide decisive, technical oversight of program activities and a high assurance of deliverable quality.

Education, Certifications, and Training

Education

- M.B.A., University of Maryland University College, (b)(6)
- M.S., Information Systems Management, University of Maryland University College, (b)(6)
- B.A., English Literature, George Mason University, (b)(6)

Certifications and Training

- Project Management Professional (PMP)
- Microsoft Certified Systems Engineer (MCSE) Windows 2000 (with Exchange)
- Microsoft Certified Systems Engineer (MCSE) Windows NT
- Polycom Certified VideoConferencing Engineer

Related Experience: Professional Career Experience

MAR, Incorporated **October 2008 – Present (3.7 years)**

Director, Cyber Security and Infrastructure Protection Programs

As the Director of Cyber Security and Infrastructure Protection Programs Mr. Simonds provides on-site program management support for the NRC. In this role Mr. Simonds has managed multiple task orders for services related to C&A, security engineering, independent verification and validation, enterprise architecture, continuous monitoring of accredited agency systems, and overall FISMA program support. He has also provided continuous organizational-level security program management services, including process development and reengineering, contingency planning, risk assessments, scanning and penetration testing, automated security tool evaluation and the presentation of executive management briefings.

Mr. Simonds has extensive experience managing integrated project plans and directing resources responsible for the development of NRC Cyber Security related regulatory policy and the performance of oversight functions. Mr. Simonds leads a specialized team of industry experts in the research, development, and implementation of Cyber Security policies and guidelines aimed at bringing nuclear power facilities within the US into compliance with NRC Cyber Security regulations. He provides Cyber Security program management support to the NRC's Office of Nuclear Security and Incident Response and Office of Nuclear Material Safety and Safeguards, takes part in licensing and policy review activities associated with initiatives under 10 CFR 73.54 and NRC cyber programs affecting its community of licensees and license applicants. Along with NRC staff, he interfaces with representatives from both the

Name:	Simonds, George A. III	Company:	MAR
Labor Category:	Program Manager	Employment Status:	Employee

nuclear power utilities and representatives from the Nuclear Energy Institute for major program activities involving Cyber Security.

He has led a team of analysts and SMEs in the review of Cyber Security plans submitted to the NRC by licensees and COL applicants that outline the programmatic framework whereby plant Cyber Security programs will be established. As a licensing support activity, he ensured adherence to regulatory guidelines for Cyber Security and the development of safety evaluation reports used by the NRC to determine whether submitted plans warrant approval by the agency. He is the organizing member of the NRC Inspection Program Working Group and supports development of NRC procedures governing how Cyber Security inspections of commercial nuclear power plants will be conducted by NRC regional inspectors. The working group consists of NRC Cyber Security program managers, inspectors, representatives from the Nuclear Energy Institute, commercial nuclear power industry, and subject matter experts from MAR and the private sector.

Mr. Simonds has supervised development of Cyber Security role-based courses and materials, and served as an instructor for executive management, IT managers, Information System Security Officers (ISSO), and system administrators. He also managed teams responsible for coordinated development (Idaho National Laboratory, Sandia National Laboratory, Pacific Northwest National Laboratory) of Cyber Security training for NRC regional inspectors.

Force 3, Inc. **July 2002 – October 2008 (6.3 years)**

Senior Engagement Manager/Project Manager

As Senior Engagement Manager/Project Manager Mr. Simonds managed more than 32 Information Assurance projects, including the C&A of 19 systems and applications. He provided ongoing systems security consulting for government clients seeking to develop, implement, and manage C&A projects for the timely authorization of major systems for operation within their respective agencies. He drafted and submitted for client acceptance key project deliverables in the form of Risk Assessments (RA), Contingency Plans (CP), and system security testing plans and their respective reports. He worked closely with the client to guide systems development through the incorporation of security measures, requirements, and controls in an effort to achieve compliance with federal guidelines. Mr. Simonds worked together with client and internal management to match qualified, talented resources to the right positions within the client's security team. He generated project plans and ensured activities remained schedule compliant throughout the certification and accreditation lifecycle. He coordinated closely with system owners and client stakeholders in the review and betterment of existing security practices and the policies that governed how security measures are implemented within their respective agencies. He planned, coordinated, and executed complex technical projects according to proven methodologies and the unique tracking, scheduling, budgeting and reporting requirements set forth within various government and commercial organizations. He provided oversight of all tasks and sub-tasks defined within the project schedule, including the coordination of internal and external resources, parallel execution of multiple activities, timely submission of agreed upon deliverables, ongoing reporting to executive sponsors, system owners, and other key stakeholders, review and remediation of schedule and budget conflicts, and relationship management between government and commercial solutions providers.

As a Senior Network Engineer he performed network health assessment surveys for small, medium, and large commercial hospitals throughout the United States in the process of implementing specialized telemedicine applications, such as critical patient monitoring and picture archive communications systems. Using non-invasive diagnostic, review, and validation approaches he provided detailed analysis of the network's integrity and remediation steps to overcome performance latencies or barriers to reliable data communications. He assisted clients in designing, implementing, and managing enterprise-wide network infrastructures to support high demand, bandwidth intensive applications in both pre and post-sales scenarios. Lastly, he worked with joint teams to develop highly specialized systems and network solutions that leverage multi-faceted technical capabilities within an integrated, seem-less architecture.

Name:	Simonds, George A. III	Company:	MAR
Labor Category:	Program Manager	Employment Status:	Employee

Information Access Solutions **July 2000 – July 2002 (2 years)**

Network Engineer

As a Network Engineer, Mr. Simonds designed, built, and maintained wireless LANs as part of an engineering team utilizing Cisco Aeronet 340 Series wireless bridges and point-to-point/omni-directional antennas, integrating 20+ sites throughout Washington DC Metro Area. He maintained and supported 100+ users LAN running WinNT 4.0 technology, to include File and Print services, DHCP, and WINS. He configured end-to-end Frame-Relay PVC's, coordinated circuit installs, and troubleshooting with telco service contractors. He produced network diagrams and relevant documentation concerning topolology changes and configuration updates for LAN and WAN devices. (Contractor – US Wireless Corporation). Mr. Simonds drafted and implemented SOP for LAN/WAN, to include training requirements, configuration standardization of desktops/servers/routers/switches/wireless bridges, and how-to manuals for remote access, SharePoint Portal Server administration, data backup, and general troubleshooting procedures. He configured and maintained Cisco 1600/1700/2500/3600 Series routers, to include EIGRP and Frame Relay. Lastly, he configured and maintained Cisco 2900, 3500, and 5500 Series switches, to include VTP, STP, and VLAN setup, and configuration of Cisco Secure PIX 506 Firewall.

UMUC, Manpower & Reserve Affairs **April 1994 – July 2000 (6.3 years)**

Department Manger/Information Systems HQ

As a Department Manager Mr. Simonds assisted 30+ office personnel as Windows 3.1 and NT Administrator, to include software/hardware installation, print services, file and data security, troubleshooting and upgrades. He acted as liaison with system administrators to ensure software/hardware requirements were satisfied, and remedied where discrepancies exist. He participated in panels designed to evaluate current IT infrastructure, and provide prospective solutions for automation support and worldwide Internet access to localized services and support agencies within Headquarters. He provided an oversight of personnel and equipment migration from department location in Arlington, VA to Quantico, VA. This involved great attention to detail, as each employee required training in Windows NT environment, filing archives required special storage facilities, and impact planning for the military base overall. He underwent extensive research analysis of policies and procedures shaped by DoD regulations, to ensure compliance with published changes both within our agency and abroad (CONUS/OCONUS).

2.1.1.2 Senior Project Manager – Thomas Evans

Name:	**Evans, Thomas E.**	**Company:**	**MAR**
Labor Category:	**Project Manager**	**Employment Status:**	**Employee**
NRC Badge:	(b)(6)	**Country of Citizenship:**	**USA**
Additional Clearance (s):			

Candidates Skills/Experience Relevant to Statement of Work

SOW #	SOW Description	Candidate Qualified
8.1	Project Management	✓
8.2	Special Projects	✓
8.3	System Authorization	✓
8.4	Continuous Monitoring Support	✓
8.5	Data Calls	✓
8.6	Cyber Situational Awareness	✓
8.7	Policy, Standards and Training	✓

Summary of Skills, Experience, and Training/Certifications Relevant to Statement of Work

Thomas Evans possesses over 15 years of progressive professional experience related to IT and Cyber Security, project management, project planning and reporting, Earned Value Management (EVM) analysis and reporting, and office systems design and implementation. Mr. Evans is PMP certified, and serves as the Project Manager for the NRC CISSS contract that encompass organization-wide security policy, standards, and training; full systems lifecycle security management; and bringing complex IT systems into compliance with the Federal Information Security Management Act of 2002 (FISMA), OMB A-130, and the National Institute of Standards and Technology (NIST) Special Publications. Mr. Evans was directly involved with the design and implementation of MAR's TaskTracker system to meet and exceed the Earned Value Management (EVM) reporting requirements of the CISSS contract in compliance with Section A-11, Part 7 of the ANSI Standard 748. Mr. Evans has strong analytical, organization, and problem solving skills, as well as excellent inter-personal communication skills which will be beneficial in his role as a Senior Project Manager for the CSPSS project.

Mr. Evans current experience as CISSS Project Manager exceeds the minimum qualifications of the Project Manager GSA Alliant Labor Category. Mr. Evans has supported the NRC for over six years in positions of progressive responsibility including his current role as Project Manager. In this role, he manages 10 subcontractors and a staff of 25-30 security professionals. He manages over 70 task orders, of which 50% or more are active at any given time. Project Manager tasks include: scheduling, budgets and spend plans, resourcing and resource allocations, customer interaction, EVM oversight using TaskTracker, problem solving, and finding innovative solutions to scheduled changes.

In his current role as Project Manager, Mr. Evans experience encompasses all area of SOW sections 8.1 through 8.7. For all task areas in the SOW, Mr. Evans is directly involved with cradle to grave project management and EVM oversight from initial task order response and award to successful delivery of all services and products. Within each of the SOW areas, Mr. Evans maintains project scheduling, customer relationships, budget and scope oversight and the direction of resources. Mr. Evans has hands on experience with all of the program offices. He has an understanding of all NRC systems and in-depth knowledge of the NRC customer through his relationships with these key personnel.

Mr. Evans experience makes him uniquely aware of the NRC mission and business objectives, and he is committed to the ongoing success of its Cyber Security program. During his tenure as a Project Manager on the CISSS contract Mr. Evans support of a variety of agency programs resulted in his possessing both an in-depth knowledge of what it takes to successfully carry out tasks and deliverables as described in Section 8 of the SOW, and positive working relationships with NRC executives, management, staff, and contractors that will promote continued improvements in these key areas.

Name:	Evans, Thomas E.	Company:	MAR
Labor Category:	Project Manager	Employment Status:	Employee

Education, Certifications, and Training

Education

- M.B.A., Hood College, (b)(6)
- B.S., Computer Science, Stratford University, (b)(6)
- A.S., Computer Science, Stratford University,

Certifications and Training

- PMP Certified, 2011
- ITIL v3 Foundation Certified, 2011
- A+ Certification, CompTIA, 2004
- Network+ Certification, CompTIA, 2004

Related Experience: Professional Career Experience

MAR, Incorporated **January 2006 – Present (6.4 years)**

Project Manager/Project Controller/Security Analyst, Information Engineer/Financial Analyst

Nuclear Regulatory Commission

Under the CISSS Contract, Mr. Evans performs the role of Project Manager where he is responsible for the management of over 70 task orders, 10 subcontractors, and 25 - 30 staff analysts for the NRC's CISSS Contract. Mr. Evans has developed strong working relationships with key NRC stakeholders. This has resulted in Mr. Evans being a trusted advisor in assisting the NRC Program Offices achieving and maintaining their Authority to Operate (ATO). In addition to managing FISMA compliance tasks, Mr. Evans has led the continued growth of other NRC Cyber Security support activities including support for the Standards Working Group, expansion of the Role-based Training including streamlining the hands-on lab support activities. Under his leadership MAR has consistently reduced the costs associated with FISMA compliance activities while often meeting compressed delivery deadlines. Mr. Evans understands the complexities in managing a diverse enterprise-wide Cyber Security contract. He has developed a forward-looking resource planning process along with the support systems to efficiently manage personnel skills, budgets, and timelines.

As Project Controller, he was responsible for maintaining the Integrated Security Activity Project Plan using Microsoft Project and Project Console, responsible for working with the Project Management Team in establishing the project plan for each task order, maintaining the integrated plan and performing EVM analysis and reporting for the NRC. Prior to his Project Manager and Project Controller duties, he was an analyst assisting Sr. Security Analysts with FISMA activities compliance at the NRC. He has performed technical writing duties for C&A at the NRC.

MAR, Incorporated, Rockville, MD

Mr. Evans manages and trains IT staff responsible for the day to day operations of the MAR office network to include the secure hardening of the infrastructure, backing up and restoring files, updating and upgrading systems, and general network maintenance. He also assists them with troubleshooting and repairing miscellaneous hardware and software errors such as network connectivity and cable failures, printing errors, and hard drive failures. Mr. Evans manages the scheduling and install of all new office and computer equipment including networking devices, servers, workstations, printers, scanners, copiers, fax machines, and other miscellaneous peripherals, when needed. He is responsible for oversight of the maintenance of MAR's Microsoft SharePoint portals.

MAR, Incorporated, Ohmsett Facility, Red Bank, NJ

He managed IT staff responsible for the network administration duties for the OHMSETT site located in Red Bank, NJ. These duties included the day to day operations of the office network including the secure hardening of the infrastructure, backup and restoration of files, system updates and upgrades, and general network maintenance.

Name:	Evans, Thomas E.	Company:	MAR
Labor Category:	Project Manager	Employment Status:	Employee

Self Employed **December 2005 – September 2010 (4.8 years)**

Information Technology Consultant

Mr. Evans worked on a part-time basis as an IT Consultant focusing on the security, installation, and repair of SOHO systems, networks, and providing digital photo repair services. He worked with the installation and troubleshooting of PCs and printers as well as miscellaneous peripherals for SOHO systems running Windows 9x/NT/XP/Vista and Linux. He worked with the installation and troubleshooting of networks using both cabled and wireless routers and switches.

State Farm **September 1998 – December 2005 (6.3 years)**

Insurance Agent/Computer Technician

As an Insurance Agent/Computer Technician at State Farm, Mr. Evans assisted clients by analyzing their needs in the areas of insurance and finance and provided them with recommendations. He installed new office and computer equipment including workstations, printers, scanners, copiers, fax machines, and other miscellaneous peripherals. He made recommendations for office and system upgrades including workstations, printers, scanners, copiers, fax machines, and other miscellaneous peripherals. He troubleshot and repaired miscellaneous hardware and software errors such as network connectivity and cable failures, printing errors, and hard drive failures. He managed office staff permissions for ECHO system, Microsoft Outlook, and shared folder access on the network. He was responsible for training staff on the use of the network, printers, and miscellaneous software that is used in day to day activities. He worked with outside vendors for the installation and repair of phone lines, T1 line, computer, and network installations when necessary. He served as Second Line Office Manager.

K-Mart Corporation **September 1994 – September 1998 (4 years)**

Manager/Hardware Technician

As a Manager of K-Mart Corporation, Mr. Evans managed a staff of fifteen employees. He helped increase Electronics Department sales by 90% through customer service and merchandising. He was responsible for creation and review of department sales reports on a weekly and monthly basis. He managed the store as on-call manager when needed. He resolved customer complaints. He maintained and repaired the photo machine, registers, and other miscellaneous office hardware.

2.1.1.3 Project Manager – Michael Bernstein

Name:	**Bernstein, Michael A.**	**Company:**	**MAR**
Labor Category:	**Project Manager**	**Employment Status:**	**Contingent Hire**
NRC Badge:	(b)(6)	**Country of Citizenship:**	**USA**
Additional Clearance (s):			

Candidates Skills/Experience Relevant to Statement of Work

SOW #	SOW Description	Candidate Qualified
8.1	Project Management	✓
8.2	Special Projects	✓
8.3	System Authorization	✓
8.4	Continuous Monitoring Support	✓
8.5	Data Calls	✓
8.6	Cyber Situational Awareness	✓
8.7	Policy, Standards and Training	✓

Summary of Skills, Experience, and Training/Certifications Relevant to Statement of Work

Mr. Bernstein possesses over four years of Project Management experience with concentration in Information Assurance, IT Risk Assessment and Automated Testing for the Department of Treasury, and Department of Homeland Security, as well as other private firms. Mr. Bernstein also has knowledge of NIST, FISMA and FISCO guidelines and has directly worked with ISSO's to make sure Cyber Security plans are compliant within these guidelines. Mr. Bernstein has strong analytical, organization, and problem solving skills, as well as excellent inter-personal communication skills.

Mr. Bernstein currently works as a Project Manager for an Information Assurance team where he manages the FMS mainframe, Certification and Accreditation Projects, and a team of ISSO's to make sure all systems are FISMA compliant. In his past experience, Mr. Bernstein has managed IT Risk Assessment teams, and an Interoperability team, as well as a team that handled Automated Testing for a private firm. He has knowledge in Test and Evaluation systems, designing, creating, scripting, running and analyzes test systems and scanning for system vulnerabilities. Mr. Bernstein is a Certified Information System Auditor, Certified in Risk System and Information System Control, a Microsoft Certified Professional, a Novell Certified Network Engineer and is ITIL Foundations Certified.

Mr. Bernstein's technical and management experience in supporting a number of Information Assurance and Cyber Security projects along with his technical certifications qualifies him to support all of the SOW areas 8.1 through 8.7. Based on the skills, experience, and certification, Mr. Bernstein will support the CSPSS as an additional Project Manager. He exceeds the minimum GSA ASB labor category requirements for a Project Manager. Mr. Bernstein has signed a letter of intent to join MAR upon receiving an NRC clearance.

Education, Certifications, and Training

Education

- (b)(6) (b)(6) B.S., Cyber Security, University of Maryland University College, (b)(6)

Certifications and Training

- ISACA – CISA – Certified Information System Auditor
- ISACA – CRISC – Certified in Risk and Information System Control
- Microsoft Certified Professional (MCP) – Windows NT 4.0, Windows 2000
- Novell Certified Network Engineer – Netware 4.0
- Information Technology Infrastructure Library (ITIL) – Foundations Certification

Name:	Bernstein, Michael A.	Company:	MAR
Labor Category:	Project Manager	Employment Status:	Contingent Hire

Related Experience: Professional Career Experience

Thompson Cobb Bazilio and Associates, PC **May 2009 – present (3 years)**

Project Manager – Information Assurance – US Treasury, Financial Management Service

As a Project Manager for the Information Assurance Group, Mr. Bernstein manages FMS mainframe and Linux audit remediation, including methodology development, project plan development, evidence creation and submission, TAF and Treasury remediation system population, system and process documentation. He has developed and presented NIST security control training for internal staff. He planned, developed and presented NIST, FISMA and FISCAM related training to Mission Assurance staff and application ISSO's. He serves as the lead liaison between FMS and Treasury OIG during yearly audits. He planned, developed and implemented Access Control remediation efforts for FIPS 199 high systems as well as advanced Mainframe Access Control concepts and theories to FMS mainframe ISSO's. He manages C&A projects for existing US Dept of Treasury, Financial Management Service (FMS) applications. He created FMS documentation for the E-RA, FIPS-199, Security Authorization, System Security Plan (SSP) and Plans of Action and Milestones (POA&Ms) processes to provide guidance and uniformity across FMS entities and applications. Mr. Bernstein conducts documentation reviews, personnel interviews, questionnaires, and hands on testing of security controls as defined by NIST SP 800-53a, Treasury and FMS specific requirements, penetration testing using industry standard tools (Nessus, Backtrack, GFI Languard) and other utilities and system risk assessments in accordance with NIST SP 800-30. He compiled test results into Security Risk Assessment and deliver to client. He recommends remediation paths for requirements that failed testing. Mr. Bernstein generated POA&M recommendations and wording for inclusion in Trusted Agent FISMA (TAF). He performed IV&V of POA&M remediation activities and advised Security Oversight on results. He manages personnel, budgets, schedules and deliverables and developed custom PHP scripts for mainframe user data parsing and reporting.

Thompson Cobb Bazilio and Associates, PC **October 2009 – December 2009 (2 months)**

Technical Project Manager – IT Risk Assessment – Network Solutions, Inc.

Mr. Bernstein managed IT Risk Assessment activities for a private industry client. He assisted the client in applying NIST guidance and baseline security controls to their environment. He performed IT Risk Assessment based on 800-53 security controls on IT infrastructure, penetration tests on external facing infrastructure and web sites and application code review for selected internally developed applications. Mr. Bernstein also compiled and analyzed results into Security Assessment Report (SAR).

Computer Aid Inc. **November 2008 – May 2009 (6 months)**

Project Manager – Automated Testing – T. Rowe Price

Mr. Bernstein managed several new and ongoing projects for client Automated and Load testing disciplines. He created and maintained detailed project plans, work breakdown structures, status reports and billing burn rates. He scouted new opportunities and develop working relationships with other departments within TRP. He developed, designed, tested and documented application load testing using HP/Mercury Load Runner as well as application regression testing using HP/Mercury Quick Test Pro (QTP). Lastly he provided mentoring and center of excellence coaching for T. Rowe Price associates and developed training curriculums regarding automated and regression testing for TRP associates.

SRA International **July 2008 – October 2008 (3 months)**

Manager

Mr. Bernstein tested and evaluated systems for compliance to Federal Security standards and guidelines (FISMA, DHS and NIST). He created full Information Assurance documentation artifacts. System Security Plans, System Test Plans, requirements traceability matrix, and system deficiency matrixes. He conducted staff interviews to document current system state. Mr. Bernstein solved technical security issues to ensure the system was compliant with policy. He scanned systems using DHS and DOD tools for system vulnerabilities. He developed and maintained detailed status updates for Government personnel. Lastly, he developed Windows and Unix hardening scripts for new systems.

Name:	Bernstein, Michael A.	Company:	MAR
Labor Category:	Project Manager	Employment Status:	Contingent Hire

WorldBridge Partners **June 2008 – July 2008 (1 month)**

Project Manager – GOMEZ Site Monitoring

Mr. Bernstein developed GOMEZ web site monitoring on over 110 different client sites. He designed, tested and implemented advanced scripted transactions to test backend availability and functionality. He designed, tested and implemented various management reports summarizing web site availability and test transaction times from various monitoring nodes across the globe. He implemented notification groups and escalation notifications based on client requirements. Lastly, he developed detailed documentation for ongoing GOMEZ administration and future enhancements.

Protegus LLC **July 2007 – May 2008 (10 months)**

Senior Performance Engineer – Department of Homeland Security

Mr. Bernstein was responsible for designing, creating, scripting, running and analyzing system load tests using Mercury/HP Load Runner using the web/http protocol. He was in charge of testing of Student and Exchange Visitor Information System via LoadRunner. Testing included scripting of 20-business process and several batch processes. He also created scripts for data seeding operations in preparation for actual load test scenarios. Mr. Bernstein performed manual testing of applications to ensure scripts are properly flowing through the application. He monitored and evaluated back-end (Oracle) performance metrics, through TOPAZ, StatsPack and other tool sets in a UNIX environment. He was in charge of testing of several new ICE SOAP services using LoadRunner. He created encrypted scripts for dealing with SSL and message level encryption of data calls. He developed, distributed and maintained detailed test plans and test summary reports. Mr. Bernstein adhered to CMMI Level 3 process and controls to ensure traceability, accountability and repeatability. He attended TRRs and RRRs. He input SCR's and TPR's when issues were found. He installed / Configured / Administered HP/Mercury Quality Center (QC). Created Users and Project within Quality center and uploaded performance scripts to the repository.

Protegus LLC **October 2003 – July 2007 (3.8 years)**

Interoperability Test Lead – Department of Homeland Security

Mr. Bernstein managed the Interoperability test team. He developed testing strategies designed to uncover security vulnerabilities and interoperability issues between different production technologies. He created Test Department Quarterly images for compliance to DHS, NIST and other federal standards as well as Test images for proper configuration against published DHS standards and Microsoft guidelines. He developed and maintained detailed testing plans and summary reports. He integrated Interoperability testing with current SLM (SDLC) processes. He attended TRR's and RRR's. He entered SCR and TPR when issues were found. He worked with Image development team to resolve issues. Mr. Bernstein performed detailed Single Sign On (SSO) vendor evaluation testing scenarios.

2.1.1.4 Financial Analyst – Rebecca Quivey

Name:	**Quivey, Rebecca E.**	**Company:**	**MAR**
Labor Category:	**Financial Analyst**	**Employment Status:**	**Employee**
NRC Badge:	(b)(6)	**Country of Citizenship:**	**USA**
Additional Clearance (s):			

Candidates Skills/Experience Relevant to Statement of Work

SOW #	SOW Description	Candidate Qualified
8.1	Project Management	✓
8.2	Special Projects	
8.3	System Authorization	
8.4	Continuous Monitoring Support	
8.5	Data Calls	
8.6	Cyber Situational Awareness	
8.7	Policy, Standards and Training	

Summary of Skills, Experience, and Training/Certifications Relevant to Statement of Work

Rebecca Quivey has worked on the CISSS contract since February 2010, providing over two years of Financial Analyst support to the MAR Project Manager and the NRC Project Officer. In her current position as Project Controller, Ms. Quivey monitors funding, spend plans, and burn rates to ensure all projects stay within scope and budget. In order to manage the financial aspects of the CISSS contract efficiently she uses MAR's TaskTracker system as well as SharePoint portals.

Ms. Quivey's experience exceeds the minimum qualifications of the GSA Alliant Financial Analyst Labor Category. Ms. Quivey currently provides support in the areas of budget, billing, reporting and financial analysis for the CISSS contract. She supports 78 task orders that include over 230 charge codes.

As Project Controller under the CISSS contract, Ms. Quivey supports the MAR Project Managers and NRC Project Officer by monitoring funding levels, spend plans and burn rates to ensure all tasks are within budget. Ms. Quivey works directly with the Project Managers to monitor staff assignments to ensure all tasks are within scope. Ms. Quivey provides resource allocations and verifies correct charging to the contract. She develops and maintains Spend Plans for all active tasks. Ms. Quivey maintains the TaskTracker system which allows MAR to manage to the ceiling, funding, and ODC level for all active Task Orders and associated subtasks. Ms. Quivey assembles responses to Contract Office requests including Technical Proposals and Cost Proposals for new Task Orders. She reviews all modifications received from the Contract Office. She develops and delivers Monthly Status Reports, Spending & Accomplishments Reports, and EVM Reports. Ms. Quivey reviews all Travel Requests for the contract to ensure proper ODC budgets. Her current experience working on the CISSS contract exceeds the financial analysis support requirements in SOW 8.1.

Education, Certifications, and Training

Education

- M.A., Communication, University at Albany, (b)(6)
- B.A., Communication Studies, SUNY Cortland, (b)(6)

Certifications and Training

- ITIL v3 Foundation Certified, 2011

Name:	Quivey, Rebecca E.	Company:	MAR
Labor Category:	Financial Analyst	Employment Status:	Employee

Related Experience: Professional Career Experience

MAR, Incorporated **February 2010 – Present (2.3 years)**

Project Controller *April 2011 - Present*

As Project Controller for the CISSS contract, Ms. Quivey works directly with the Project Officer to monitor funding levels, spend plans, and burn rates to ensure all tasks are within budget. She also works directly with the Project Manager to monitor staff assignments to ensure all tasks are within scope. She provides resource allocations and verifies correct charging to the contract. She develops and maintains Spend Plans for all active tasks. She maintains the TaskTracker system which allows MAR to manage to the ceiling, funding, and ODC level for all active Task Orders and associated subtasks. She assembles responses to Contract Office requests including Technical Proposals and Cost Proposals for new Task Orders. She reviews all modifications received from the Contract Office. She develops and delivers Monthly Status Reports, Spending & Accomplishments Reports, and EVM Reports. She reviews all Travel Requests for the contract to ensure proper ODC budgets.

Project Administrator *February 2010 – March 2011*

As Project Administrator under the CISSS contract, Ms. Quivey assisted the Project/QA Managers in monitoring all tasks and deliverables on the CISSS Contract. She developed and maintained a MAR SharePoint Dashboard to create greater efficiency in managing over 20 active Task Orders. She developed a Weekly Deliverable Report and Accomplishments list. Ms. Quivey developed Project Plans using Microsoft Project for all Authorizations, Continuous Monitoring and Special Projects. She developed Weekly and Monthly Status Reports. She tracked iLearn Security Training completion for CISSS contractors. Ms. Quivey hosted webinars on GoToMeeting for Cyber Security Training. She assisted the Project Controller with managing financial activities on the CISSS Contract.

New York State Association of Counties **September 2008 – December 2008 (3 months)**

Media Relations Intern

As a Media Relations Intern, Ms. Quivey developed and pitched press releases to state wide media outlets, tracked media coverage, edited association's quarterly publication NYSAC News, and updated website content using Macromedia Contribute.

2.1.1.5 Administration/Clerical (Senior) – Lauren Dickman

Name:	**Dickman, Lauren E.**	**Company:**	**MAR**
Labor Category:	**Administration/Clerical (Senior)**	**Employment Status:**	**Employee**
NRC Badge:	(b)(6)	**Country of Citizenship:**	**USA**
Additional Clearance (s):			

Candidates Skills/Experience Relevant to Statement of Work

SOW #	SOW Description	Candidate Qualified
8.1	Project Management	✓
8.2	Special Projects	
8.3	System Authorization	
8.4	Continuous Monitoring Support	
8.5	Data Calls	
8.6	Cyber Situational Awareness	
8.7	Policy, Standards and Training	

Summary of Skills, Experience, and Training/Certifications Relevant to Statement of Work

Lauren Dickman possesses four years of administrative experience supporting lead management with day-to-day administrative duties and tasks. Of her four years, Ms. Dickman has spent the last year supporting the CISSS contract Project Managers. Her duties include developing reports, updating various project management sites, and attending daily meetings with customers.

Ms. Dickman's experience exceeds the minimum qualifications of the Administration/Clerical GSA Alliant Labor Category. Ms. Dickman is responsible for drafting and editing key documents in support of CISSS contract requirements. She interfaces with employees, subcontractors and customers to coordinate meetings, maintain logs, update files in SharePoint and provide general administrative support. Ms. Dickman is also responsible for maintaining operations documentation, status reports, and security related information.

On a daily basis Ms. Dickman receives specific direction and guidance from MAR Project Managers related to Administrative tasks that must be completed under this contract in a timely manner. Ms. Dickman tracks the progress and completion of project deliverables. In addition, she develops weekly and monthly status reports for the customer and updates TaskTracker with all technical completion information. Her current experience working on the CISSS contract qualifies her to both meet and exceed the duties required under SOW 8.1 for this position.

Education, Certifications, and Training

Education

- B.S., Psychology, Radford University. (b)(6)

Certifications and Training

- Service Contract Act Training, 2009

Related Experience: Professional Career Experience

MAR, Incorporated — **May 2008 – Present (4.1 years)**
Project Administrator — *May 2011 - Present*

Ms. Dickman supports the CISSS contract for the NRC in the role of Project Administrator. She supports the Project Manager on this contract in managing all phases of the project management process for the Information Assurance program at the NRC. She assists the Project Controller and Project Manager while ensuring that projects are completed on-time and within scope and budget. Ms. Dickman tracks the progress and completion of project deliverables. She develops Weekly and Monthly Status Reports for the customer. She assists the Facility Security Officer (FSO) with the personnel badge process. Ms. Dickman tracks iLearn Accounts, assists new hires with NRC account activation and employee set up, and updates TaskTracker with Technical Completion.

Name:	Dickman, Lauren E.	Company:	MAR
Labor Category:	Administration/Clerical (Senior)	Employment Status:	Employee

Human Resources Specialist *May 2008 – May 2011*

As Human Resources Specialist, Ms. Dickman performed cradle to grave Human Resources administrative duties and tasks related to: recruitment, hiring, benefits, ISO 9001:2008, and new hire on-boarding. Included in these areas Ms. Dickman performed the following specific tasks: recruited for the company in all business areas including: IT, Engineering, Administrative, and Intelligence, scheduled interviews and provided follow-up information to candidates, updated and maintained the corporate resume database, managed all recruitment job postings which included: Monster.com, CareerBuilder, Washington Post, and the MAR website, developed position descriptions for all new hires, assisted in proposal process by recruiting for candidates, formatted resumes, prepared contingent offer letters, and prepared Skills Matrix Charts, completed salary surveys and/or other employee informational surveys as needed. She tracked employee referrals for the company Employee Referral Incentive Program, processed new hire paperwork, tracked all new hire and benefit information, answered questions related to benefits, calculated and submitted all monthly benefit bills to Accounts Payable, which included health insurance, dental insurance, vision insurance, life insurance, long-term disability insurance and 401(k), tracked COBRA benefits. She was responsible for tracking and processing all Flexible Spending, and was responsible for processing and tracking all Workers Compensation claims. She received SCA training and was a member of the Professional Services Council, Labor Relations Committee.

2.1.2 Quality Assurance Team

2.1.2.1 Subject Matter Expert (Senior) – Hank Williams

Name:	**Williams, Hank**	**Company:**	**KCG**
Labor Category:	**Subject Matter Expert (Senior)**	**Employment Status:**	**Employee**
NRC Badge:	(b)(6)	**Country of Citizenship:**	**USA**
Additional Clearance (s):			

Candidates Skills/Experience Relevant to Statement of Work

SOW #	SOW Description	Candidate Qualified
8.1	Project Management	✓
8.2	Special Projects	✓
8.3	System Authorization	✓
8.4	Continuous Monitoring Support	✓
8.5	Data Calls	✓
8.6	Cyber Situational Awareness	✓
8.7	Policy, Standards and Training	✓

Summary of Skills, Experience, and Training/Certifications Relevant to Statement of Work

Hank Williams possesses more than 15 years of information systems experience, including more than 12 years of information security experience. He is currently serving as the Senior Cyber Security Engineer and Program Panager with the Financial Management Service of the Department of the Treasury. He has previously served in that same capacity regarding Cyber Security efforts with: IT Services Division at the Federal Bureau of Investigation, the Nuclear Regulatory Commission, the Foreign Terrorist Tracking Task Force/FBI, the Executive Office United States Attorneys/Department of Justice, and the Federal Emergency Management Agency/Department of Homeland Security.

Mr. Williams will serve as the Technical QA Team Lead and is considered an expert in Cyber Security having obtained multiple certifications and a graduate degree in Information Assurance. His over 15 years of Information Systems experience exceeds the requirements related to the SME (Senior) Alliant GSA Labor Category. His expertise in the industry led to his selection as an adjunct professor within the Cyber Security Master's Program at UMUC, and therefore serves as a SME in this related field. Mr. Williams has either led or performed activities within all phases of the Information Assurance Risk Management Framework and has been responsible for the successful accreditation of many high level systems that are vital to national security. He is a trusted advisor to senior level executives within several departments of the Federal Government and is highly regarded for his programmatic counsel on Cyber Security issues.

Mr. Williams has more than eight years of experience in Project Management leading complex tasks in information security. He possesses more than 12 years of experience in all phases of the C&A process and creation and review of System Security documentation and system authorization. Mr. Williams conducts risk assessments of enterprise IT systems and develops strategies for mitigating vulnerabilities. He develops security policies and plans for Disaster Recovery, Incident Response, and Physical and Environmental Security. He has developed, reviewed, implemented, coordinated and provided recommendations on security policies and procedures in multiple Government Agencies.

Education, Certifications, and Training

Education

- M.B.A., Business Administration, University of Maryland University College (b)(6)
- M.S., Computers Systems Management/Information Assurance, University of Maryland University College, (b)(6)
- B.S., Information Technology/Database Management, University of Phoenix, (b)(6)

Name:	Williams, Hank	Company:	KCG
Labor Category:	Subject Matter Expert (Senior)	Employment Status:	Employee

Certifications and Training:

- PMP, Project Management Institute, 2008
- CISM, ISACA (formerly-Information Systems Audit and Control Association), 2008
- CISSP, International Information Systems Security Certification Consortium $(ISC)^2$, 2004
- GLEG, Global Information Assurance Certification (SANS), 2011
- Masters Certificate in Project Management – University of Maryland University College, 2008

Related Experience: Professional Career Experience

Knowledge Consulting Group, Inc. **September 2003 – Present (8.8 years)**

Subject Matter Expert/Program Manager

Project Team Lead for multiple contract vehicles that produce over $3 million in annual revenue. Responsible for concurrent management of multiple complex task areas and oversight of all project deliverables, project financial obligations, and burn rate. Manage a diverse team responsible for performing the following enterprise wide tasks across multiple security domains. Investigate new lines of business and develop partnerships with outside companies to increase revenue and market share.

Specific Tasks/Deliverables Completed:

- Maintain company and client level executive accountability and reporting, ensuring the overall success of all assigned contracts and task areas.
- Serve as trusted advisor to executive level government managers on all aspects of Cyber Security within various departments of the Federal Government. Provide guidance on all aspects of the Risk Management Framework as mandated by the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST).
- Manage information assurance services to maintain the security C&A of network systems including, but not limited to, scheduling and attending periodic meetings with the FBI Security Division to review the security requirements, resolve any issues and provide updates relevant to the SSP and the C&A process.
- Manage security engineering services to ensure that the network designs remain secure and that the security C&A is not compromised by any changes that are made to the system.
- Manage support for Security Tests and Evaluations and Computer and/or Network Forensics.
- Develop solutions in response to Requests for Proposal for Cyber Security line of business with multiple agencies within the Federal Government.

Recent engagements within Knowledge Consulting Group include:

Financial Management Service/Department of the Treasury January 2012 – Present (6 months)

Subject Matter Expert/Program Manager

Specific Tasks/Deliverables Completed:

- Provide SME level support to the IT Security Oversight and Compliance Branch
- Review SA&A Documentation for compliance with NIST requirements
- Schedule ST&E testing Activities
- Review, develop and present training in support of the FMS ISSO program

Information Technology Services Division/FBI October 2009 – December 2011 (2.2 years)

Subject Matter Expert/Program Manager

Project Team Lead supervising a 20 personnel team charged with providing enterprise security services across multiple enclaves in three task areas; ISSO support, Vulnerability Management and Enterprise Account Management.

Specific Tasks/Deliverables Completed:

- Led team of ISSOs providing support to enterprise backbone systems across 3 security enclaves. Systems comprised over 100,000 workstations and servers worldwide.
- Led vulnerability management team responsible for maintaining enterprise anti-virus solution across 3 security enclaves. Also responsible for managing data spill incidents within these enclaves.

Name:	Williams, Hank	Company:	KCG
Labor Category:	Subject Matter Expert (Senior)	Employment Status:	Employee

- Led enterprise account management team responsible for all account activities within both Windows Active Directory and IBM mainframe across 3 security enclaves. Responsible for developing and testing group policy objects within these enclaves.
- Personally served as senior Cyber Security advisor to SES level executives within the IT Services Division.

Nuclear Regulatory Commission October 2008 – October 2009 (1 year)
Subject Matter Expert/Program Manager
Provided direct support to the NRC Chief Information Security Officer by serving as the Subject Matter Expert for Information Assurance. On-site manager and business leader with supervisory oversight of personnel.
Specific Tasks/Deliverables Completed:

- Providing recommendations on Security Categorization Documents and the C&A packages of unclassified systems according to Federal and NRC regulations, guidelines, and standards.
- Providing recommendations on C&A packages of classified systems according to guidance provided by the Committee on National Security Systems (CNSS).
- Providing recommendations on Capital Planning and Investment Control (CPIC) Screening Form and Business Case Packages.
- Providing recommendations on all FISMA related deliverables (Contingency Plans, Contingency Test Reports, Plan of Action & Milestone (POA&M) Reports, etc.).
- Providing recommendations on the Organization's C&A process and security program to ensure federal regulations, guidelines, and standards are being met.
- Developing evaluation criteria and procedures for approval to ensure that systems are evaluated in a similar manner from one review to the next.
- Assisting the agency in responding to data calls from the Office of the Inspector General (OIG), Office of Management and Budget (OMB), and other government agencies.
- Analyzing IT security best practices to determine how they can be applied at NRC.

Foreign Terrorist Tracking Task Force/FBI February 2007 – October 2008 (1.6 years)
Sr. Cyber Security Engineer/Program Manager
On-site manager and business leader with supervisory oversight of 11 personnel. Also serve as the InfoSec Team Lead for six-person shop
Specific Tasks/Deliverables Completed:

- Led InfoSec shop responsible for ISSO and Security Engineer duties on 3 major systems.
- Personally served as senior Cyber Security advisor to the task force Director.

Corporate Lodging Corporation/FEMA August 2006 – December 2007 (1.3 years)
Sr. Network Security Engineer/Program Manager
Project Manager of a team of Information Assurance engineers performing Certification and Security Testing and Evaluation of a corporate client based upon requirements mandated from their contract with FEMA.
Specific Tasks/Deliverables Completed:

- Assisted CLC in establishing an Information Security Program by generating applicable policies and plans, including a Contingency and Disaster Recovery Policy and Plan and develop methodologies and plans for applying security configurations and mitigating actions.
- Performed an initial discovery effort and risk assessment to determine system boundaries followed by the creation of a strategy to best accomplish the system certifications IAW NIST Guidelines.
- Determined Information Categories and sensitivities IAW NIST 800-60 resulting in an overall FIPS 199 Impact levels being assigned to the system.
- Identified applicable security controls and developed test procedures based upon industry accepted

Name:	Williams, Hank	Company:	KCG
Labor Category:	Subject Matter Expert (Senior)	Employment Status:	Employee

best practices to ensure secure system operation.

- Tested systems by technical methods such as scanners (HarrisStat, Web Inspect, etc) CIS Configuration Scripts, both automated and manual, and interviews with FEMA personnel.
- Prepared a final Security Evaluation Report and a certification recommendation which was submitted to the Designated Approval Authority once testing was completed and all mitigating actions were validated.
- Entered unmitigated findings into a Plan of Actions and Milestones (POA&M).

Executive Office United States Attorney/DOJ October 2005 – April 2006 (7 months)
Sr. Network Security Engineer/Team Leader
Team leader of a matrixed team of Information Assurance engineers performing Certification and Security Testing and Evaluation of an EOUSA system.
Specific Tasks/Deliverables Completed:

- Performed an initial discovery effort to determine system boundaries followed by the creation of a strategy to best accomplish the system certifications IAW NIST and Department of Justice Guidelines.
- Determined Information Categories and sensitivities IAW NIST 800-60 resulting in an overall FIPS 199 Impact level being assigned to the separate systems.
- Identified applicable security controls and developed test procedures based upon industry accepted best practices to ensure secure system operation.
- Performed multiple rounds of testing, presented findings to client and provided assistance to the client in determining methods to mitigate the vulnerabilities.
- Developed final risk analysis with a certification recommendation based upon the risk analysis.
- Accomplished the full certifications of 3 networks.
- Worked with a new EOUSA entity to develop required policies and plans, such as Configuration Management, Contingency and Disaster Recovery, Incident Response, Security Awareness and Training, and Physical and Environmental Security.

Knowledge Consulting Group, Inc. September 2003 – October 2005 (2.1 years)
Sr. Network Security Engineer/Team Leader
Certification Lead for FBI Information Assurance Certification Unit. Team Leader of matrixed Certification and Accreditation team on FBI Information Systems.
Specific Tasks/Deliverables Completed:

- Planned and developed strategies for security implementation. Reviewed SSPs, Concept of Operations (CONOPS) and other security documentation on information systems for completeness and accuracy.
- Coordinated with System Owners and Accreditation staff to determine security levels and postures during system development.
- Determined Security Requirements by preparation of the Security Requirements Traceability Matrix based upon applicable Federal Government, Department of Justice, and FBI regulations.
- Conducted risk and vulnerability assessments of planned and installed information systems to identify vulnerabilities, risks, and protection needs.
- Assisted system owners in formulating strategies for risk reduction based upon applicable regulations and industry best-known practices.
- Made certification recommendations based upon the security posture and residual risk levels of information systems.
- Acted as overall Certification Team lead in the absence of the government team lead.

Name:	Williams, Hank	Company:	KCG
Labor Category:	Subject Matter Expert (Senior)	Employment Status:	Employee

Joint Interagency Task Force West (JIATF-W) **June 2002 – August 2003 (1.2 years)**

Information Systems Security Manager

Responsible for all Information Security/Information Assurance Issues and supervision of staff personnel.

Specific Tasks/Deliverables Completed:

- Developed new C&A documentation for all major IT related systems leading to systems being granted Authority to Operate (ATO).
- Developed System Security Authorization Agreements (SSAA) for internal migration upgrade from Windows NT to Windows 2000.
- Performed Security testing on Windows 2000 LAN.
- Implemented and managed entire Public Key Infrastructure for JIATF-W and coordinated all PKI issues with the Defense Intelligence Agency to receive certificates.
- Developed Information Conditions (INFOCONs) as directed by the Theater Commander to allow information protection based on a specific level of need.

Western Army Reserve Intelligence Support Center **July 1999 – June 2002 (2.9 years)**

Systems Administrator/Special Security Officer

Senior Systems Administrator for entire Windows NT and UNIX network.

Specific Tasks/Deliverables Completed:

- Information Systems Security Officer responsible for ensuring assigned systems were configured IAW applicable regulations and guidelines.
- Responsible for ensuring all system documentation is complete and prepared IAW DITSCAP and other requirements.
- Selected to participate in the development of the Advanced System Administrator course at National Headquarters.
- Responsible for all levels of support including Workstations, Servers, and all internal Network configurations.

Defense Intelligence Agency (DIA) Defense Attache System September 1994 – July 1999 (4.8 years)

Operations Non-Commissioned Officer

Assigned to oversee IT operations in offices in Mexico City, Mexico and Manila, Republic of the Philippines

Specific Tasks/Deliverables Completed:

- Responsible for all office automation and local network support in both offices.
- Developed a series of macros for automating monthly reports later adopted by other offices in the Defense Attaché' System.
- Supervised foreign national workforce of between four and eight employees.

2.1.2.2 Quality Assurance Specialist (Journeyman) – Sandra Smith

Name:	**Smith, Sandra S.**	**Company:**	**MAR**
Labor Category:	**Quality Assurance Specialist (Journeyman)**	**Employment Status:**	**Consultant**
NRC Badge:	(b)(6)	**Country of Citizenship:**	**USA**
Additional Clearance (s):			

Candidates Skills/Experience Relevant to Statement of Work

SOW #	SOW Description	Candidate Qualified
8.1	Project Management	✓
8.2	Special Projects	✓
8.3	System Authorization	✓
8.4	Continuous Monitoring Support	✓
8.5	Data Calls	
8.6	Cyber Situational Awareness	✓
8.7	Policy, Standards and Training	✓

Summary of Skills, Experience, and Training/Certifications Relevant to Statement of Work

Sandra Smith has more than 15 years of experience providing technical writing/editing support. Documentation experience encompasses: Program Management - including business process reengineering (BPR), change management, Quality Assurance/Control (QA/QC), and Capital Planning and Investment Control (CPIC); System Development - including user and maintenance manuals, training materials, database design, configuration management, and requirements specifications; and Systems/Information Security - including development and coordination of security procedures, policies, and documentation supporting system C&A.

Ms. Smith's 15 years of experience in Technical Writing and Quality Assurance exceeds the minimum qualifications of the Quality Assurance Specialist (Journeyman) GSA Alliant labor category. As the president of TDS Writing Solutions, Inc., Ms. Smith has developed end user guides for each version of the application deployed, providing QA/QC reviews of application screens. She has provided editorial support for multiple agencies for system security and lifecycle documentation to ensure compliance with the National Institute of Standards and Technology (NIST) Federal Information Processing Standards Publication 201 (FIPS PUB 201). She has also developed IT security policies and standard operating procedures in accordance with TD P 85-01 and NIST for C&A of TIGTA's enterprise network and telecommunications infrastructure.

Ms. Smith's over 15 Quality Assurance years of experience exceeds the requirements in SOW areas 8.1, 8.2, 8.3, 8.4, 8.6 and 8.7. Her experience includes Program Management - including business process reengineering (BPR), change management, quality assurance/control (QA/QC), and Capital Planning and Investment Control (CPIC). System Development - including user and maintenance manuals, training materials, database design, configuration management, and requirements specifications. Also, she has Systems/Information Security - including development and coordination of security procedures, policies, and documentation supporting system C&A. Ms. Smith will be brought in to assist with high level tasks and deliverables as determined by the NRC customer.

Education, Certifications, and Training

Education

- B.S., Economics, Radford University, (b)(6)

Name:	Smith, Sandra S.	Company:	MAR
Labor Category:	Quality Assurance Specialist (Journeyman)	Employment Status:	Consultant

Related Experience: Professional Career Experience

TDS Writing Solutions, Inc. **2003 – Present (9 years)**
President

Ms. Smith provides services to private corporations and federal agencies and departments through prime contractors. In support to FBCS, a small non-profit organization, Ms. Smith performs the following tasks: developing and publishing monthly multi-page newsletter, and analyzing and updating documentation structure supporting organization processes.

In support to Protiviti Government Solutions (PGS) Ms. Smith provided documentation development support on significant business transformation efforts at the Internal Revenue Service (IRS) and the Securities and Exchange Commission (SEC) that encompass the development of strategic recommendations for the reorganization and BPR of programs and systems based on the Six Sigma DMAIC methodology.

In support to Modis, Inc. at Electronic Data Systems (EDS) for the EDS Assured Identity™ system that produces Personal Identity Verification (PIV) credentials in support of Homeland Security Presidential Directive 12 (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors Ms. Smith performed the following tasks: developed end user guides for each version of the application deployed, providing QA/QC reviews of application screens, and provided editorial support for system security and lifecycle documentation to ensure compliance with the National Institute of Standards and Technology (NIST) Federal Information Processing Standards Publication 201 (FIPS PUB 201).

In support to Innovative Management & Technology Approaches, Inc. (IMTAS) at the Treasury Inspector General for Tax Administration (TIGTA) Ms. Smith developed policies, procedures, and on-line training materials in support of implementing HSPD-12 and FIPS 201 into the organization and returned for annual update of IT security policies and standard operating procedures for TIGTA's enterprise network and telecommunications infrastructure, to ensure compliance with the Department of the Treasury's IT Security Program (TD P 85-01) and NIST. Originally developed these security policies for (1) the submission to the annual Treasury Security Program Review of TIGTA and (2) TIGTA achieving C&A.

In support to P2C2 Group, Inc. Ms. Smith provided oversight and editorial support to the Federal Reserve Bank of Richmond (FRBR) on the Intra-Governmental Payment and Collection (IPAC) project to meet Office of Management and Budget (OMB)/CPIC process reporting requirements (i.e., Exhibit 300/53, Dashboards, and Operational Analysis), developed an Operational Analysis for the Department of Education (ED) for the Migrant Student Information Exchange (MSIX) system which was mandated by Congress to support the No Child Left Behind (NCLB) Act, and provided oversight and editorial support to the U.S. Agency for International Development (USAID) in the CPIC process for the development of two business cases for the OMB Exhibit 300s. Coordinated development of business cases with USAID Project Managers from each business area and collected data for inclusion in the OMB Exhibit 300s. Ms. Smith has also provided editorial support to the Federal Law Enforcement Training Center (FLETC), a component of the Department of Homeland Security (DHS), on documentation exploring the potential for developing a digital learning capability (e-Learning) to support residential and non-residential training of law enforcement officers, and provided editorial support to the U.S. Department of Agriculture (USDA) on three contracts in the Natural Resources Conservation Service (NRCS), based in Ft. Collins, CO. Completed editorial reviews on the Exhibit 300's developed under each contract in support of the CPIC process. She has provided editorial support to the Civil Rights Division of USDA in the CPIC process for the OMB Exhibit 300 for implementation and deployment of a new Civil Rights Enterprise System (CRES). The supporting documentation included a Requirements Analysis, Cost Benefits Analysis/Alternatives Analysis, Risk Management and Mitigation Plan, and an Enterprise-wide Implementation Project Management Plan.

Name:	Smith, Sandra S.	Company:	MAR
Labor Category:	Quality Assurance Specialist (Journeyman)	Employment Status:	Consultant

In support to MicroLink, LLC, Ms. Smith developed a process guide for the Huron Consulting Group's e-discovery solution, V3locityTM. This litigation support initiative offers law firms, corporate legal departments, and government agencies a streamlined approach to respond quickly and defensibly to legal and investigative requests for electronic evidence, and provided editorial support on existing documentation for MS SharePoint customization projects (i.e., training materials for the Naval Criminal Investigative Service (NCIS).

In support to K4 Solutions, Inc, Ms. Smith developed and maintained IT security and system documentation for C&A of the imaging systems at the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) and the Alcohol and Tobacco Tax and Trade Bureau (TTB). Security documentation included a Security Plan, Risk Assessment, Contingency Plan, Minimum Security Requirements, and Application Security Inventory. Also in support of these imaging systems, developed the ATF/TTB Imaging Systems – System Overviews document to briefly detail the purpose, workflow, architecture, process flow, and points of contact for each of the imaging systems currently implemented within ATF and TTB. Ms. Smith provided editorial support to the Office of the Assistant Secretary for Administration and Management (OASAM) at the Department of Labor (DOL) in finalizing documentation for the implementation of a shared Public Key Infrastructure (PKI) as part of an overall security strategy to secure DOL's information and networked computer-based systems. This documentation included the Certificate Policy for the Certification Authority, Certification Practice Statement, Detailed Design Document, Concept of Operations, and DOL Policy for Public Key Infrastructure.

In support to Orizon, Inc., Ms. Smith provided editorial support on processes and standards at the Financial Management Domain (FMD) of the Office of the Under Secretary of Defense (Comptroller) (OUSD(C)) for the Business Modernization Program, and provided editorial support to the Department of Housing and Urban Development (HUD) Federal Housing Authority (FHA) Loss Mitigation Program on the Loss Mitigation Analysis Report.

Self-Employed **1999 – 2003 (4 years)**

Ms. Smith provided subcontract services to Federal Agencies and departments through prime contractors. In support to Business Integrated Technology Solutions, Inc. (BITS) at TIGTA Ms. Smith developed IT security policies and standard operating procedures in accordance with TD P 85-01 and NIST for C&A of TIGTA's enterprise network and telecommunications infrastructure. Deliverables consisted of 30 IT security policies, a Continuity of Operations Plan (COOP) revision, a Configuration Management Plan (CMP) and presentation on implementing CM into the organization, a System Security Authorization Agreement (SSAA), and a TIGTA Communication Data Network Security Plan.

In support to JV Mason & Associates, Inc. (JVMA) at the Procurement Systems Division (PSD) of the Office of Procurement and Property Management (OPPM) at USDA Ms. Smith developed a CMP for the USDA Purchase Card Program and assisted in implementing configuration management into the program with the goal to achieve SEI CMM Level 2 certification. She also developed and maintained program, system, and operational documentation, user manuals, training materials, and installation guides for the Purchase Card Management System (PCMS), forms, brochures, slides, and other presentation aids and exhibits for PCMS. She executed quality assurance software tests on two version releases of PCMS and evaluated results to ensure compliance with applicable regulations and conducted PCMS user studies; database cleanup; and evaluation of system functionality, ease of use, efficiency, and accuracy.

DynCorp I&ET **1997 – 1998 (2 years)**
Senior Technical Writer/Subcontract Task Lead

As technical writing support to team members pursuing EC/EDI for the exchange of tax and wage data on the Simplified Tax and Wage Reporting System (STAWRS) Project under the Treasury Information Processing Support Services (TIPSS) contract, Ms. Smith developed SDLC documentation ranging from project planning and configuration management to system requirements and development. She

Name:	Smith, Sandra S.	Company:	MAR
Labor Category:	Quality Assurance Specialist (Journeyman)	Employment Status:	Consultant

performed as Task Lead for subcontract with Price Waterhouse Coopers to oversee the development of a survey to distribute to employers for input in determining ways of easing their tax-reporting burden by modifying their methods of filing tax and wage reports. This project was SEI CMM Level 2 certified.

Sterling Software **1995 – 1996 (1 year)**
Documentation Team Leader

As Team Leader for the Documentation Staff on the Modernized Integrated Database (MIDB) Project, Ms. Smith managed and trained all members of the staff, created the MIDB Documentation Style Guide, provided a variety of documentation status reports, and ensured the timely completion and accuracy of all documentation deliverables. The Documentation Staff was responsible for creating and updating all system lifecycle documents stipulated in the statement of work (SOW) and writing training courseware, user guides and manuals, and test plans.

McClendon Automation **1992 – 1995 (3 years)**
Senior Technical Writer

As technical documentation support for the Programming and Execution (PAX) Support Office of the U.S. Army Corps of Engineers, Ms. Smith developed system software and database maintenance manuals, online helps, and user manuals for FOCUS database systems, Construction Appropriations Programming, Control, and Execution Systems (CAPCES) subsystems, and the Directives Network (DIRNET) database. She interfaced with subject matter experts in developing all documentation. In addition to documentation support, Ms. Smith redesigned the PAX Hotline database using ACCESS and assisted in the design and development of both the Knowledge Worker System (KWS) database using Visual Basic and the DIRNET database using ACCESS.

SYSCON Corporation **1990 – 1992 (2 years)**
Senior Analyst/Technical Writer

Ms. Smith provided technical documentation support for a national minicomputer network in the Civil Division of the Department of Justice (DOJ). She documented and tested programs designed and developed for use in system management and performance. Ms. Smith also edited and updated procedure manuals for an ORACLE Hotline database and assisted programmers with the development of ORACLE applications. Ms. Smith developed user manuals for ORACLE database applications and AS/400 backup procedures. She also developed database training course materials and conducted training for mainframe and PC applications for both technical and non-technical personnel of the Civil Division.

2.1.2.3 Quality Assurance Specialist (Journeyman) – Deborah Pollack

Name:	**Pollack, Deborah L.**	**Company:**	**MAR**
Labor Category:	**Quality Assurance Specialist (Journeyman)**	**Employment Status:**	**Employee**
NRC Badge:	(b)(6)	**Country of Citizenship:**	**USA**
Additional Clearance (s):			

Candidates Skills/Experience Relevant to Statement of Work

SOW #	SOW Description	Candidate Qualified
8.1	Project Management	✓
8.2	Special Projects	✓
8.3	System Authorization	✓
8.4	Continuous Monitoring Support	✓
8.5	Data Calls	
8.6	Cyber Situational Awareness	✓
8.7	Policy, Standards and Training	✓

Summary of Skills, Experience, and Training/Certifications Relevant to Statement of Work

Deborah Pollack possesses over 25 years of professional experience in the areas of Technical Writing, Quality Assurance (QA) and Publications. Throughout her career, Ms. Pollack has served as a lead technical writer, writing, editing and publishing user manuals, data sheets, marketing collateral, testing manuals, and publication style guides. In addition, Ms. Pollack has conducted on-sight training related to strategic communications. Ms. Pollack has developed numerous templates using various software applications in order to assure quality assurance and consistency in all deliverables.

Ms. Pollack will support the QA Team Technical Lead. Her current experience as Quality Assurance Manager on the CISSS contract and her 25 years of experience exceeds the minimum qualifications of the Quality Assurance Specialist (Journeyman) GSA Alliant Small Business labor category. Under the CISSS contract, Ms. Pollack is responsible for defining, developing, and deploying a quality process for all MAR CISSS contract deliverables. She is responsible for supervising QA colleagues, scheduling QA activities, and delivering accurate documentation to the NRC. She has had experience as a Publications Lead for three engineering sites, supervised the development and production of user documentation, electronic user assistance, and business process documents. She has established efficient business practices and improved the quality of publications deliverables through the implementation of checklists, automated processes, and template enhancements. Ms. Pollack has managed the translation of product manuals into seven languages, and supervised translation contractors to ensure delivery of accurate materials to our global customer base.

For the CISSS contract, Ms. Pollack acts as the leader of the QA Team and has implemented best practices and established standard repeatable processes to ensure delivery of accurate information security policy, guidance, and authorization documentation. The role of QA touches every SOW area as each task requires accurate and on time deliverables for the NRC customer and Ms. Pollack will play a key role in supporting the technical teams. She will continue to be responsible for defining, developing, and deploying quality contract deliverables. Ms. Pollack's skills and hands on QA experience working on the CISSS contract qualifies her to provide QA support for SOW areas 8.1, 8.2, 8.3, 8.4 and 8.7.

Education, Certifications, and Training

Education

- Hearing and Speech coursework, University of Maryland, (b)(6)
- Hearing and Speech coursework, Rochester Institute of Technology, (b)(6)

Certifications and Training

- ITIL, Version 3, May 2011
- Project Management Essentials, 24 PDUs for PMP, January 2010

Name:	Pollack, Deborah L.	Company:	MAR
Labor Category:	Quality Assurance Specialist (Journeyman)	Employment Status:	Employee

- WinHelp Development Training, Sageline Publishing, 1994
- HTML Help Training, Sageline Publishing, 1995
- Progress 4GL Training, 1990

Related Experience: Professional Career Experience

MAR, Incorporated **August 2010 – Present (1.8 years)**

Quality Assurance Manager

As a QA Manager under the CISSS contract, Ms. Pollack is responsible for defining, developing and deploying a quality process for all MAR CISSS contract deliverables. She is responsible for supervising QA colleagues, scheduling QA activities, and delivering accurate documentation to the NRC.

As a Technical Writer under the CISSS contract, Ms. Pollack wrote, reviewed, and edited information security policy, guidance, and authorization documentation in support of the MAR CISSS contract with the NRC. She developed quality assurance checklists and procedures to ensure consistency throughout all deliverables.

JDS Uniphase **2001 – August 2010 (9 years)**

Publications Lead/Technical Writer III

As a Publications Lead/Technical Writer III, Ms. Pollack developed Getting Started Manuals, Testing Manuals, and HTML help for portable telecommunications test instruments using Adobe FrameMaker. She improved business practices through implementation of publication schedules, documentation plans, peer reviews, editing checklists, and prepress checklists. She supervised a team of writers located in multiple sites supporting up to ten concurrent engineering projects. She supported engineering projects in the US, Germany, and China. Ms. Pollack published a Request for Proposal for user interface string and documentation translations. She worked with stakeholders to evaluate proposals, select qualified agencies, and ensure that translated strings and documents were reviewed for accuracy before publication. Ms. Pollack facilitated the migration to USB delivery of PDFs by establishing standards and processes with their Quality, Manufacturing, and Operations organizations. She supervised contractors supporting Service Manual development for military contracts.

MEI Software Systems **1992 – 2001 (9 years)**

Strategic Communications Writer

As a Strategic Communications Writer, Ms. Pollack served as lead technical writer supporting the company's association management software applications. She designed templates using WordPerfect and automated the conversion of legacy documents using customized macros. Ms. Pollack designed templates for online and context-sensitive help using RoboHELP Classic and RoboHELP HTML. She developed a Publication Style Guide to be used by the technical writing group and contractors. She wrote and used procedures to test the software applications and debugged applications written in Progress 4GL.

Design Data Systems **1986 – 1992 (6 years)**

Technical Writer/Trainer/Quality Assurance Technician

As a Technical Writer/Trainer/Quality Assurance Technician, Ms. Pollack supported launch of a new Association Management Database (DATASYS4). She designed the template for task-based user manuals supporting each application module. Ms. Pollack wrote, edited, and published user manuals, data sheets, and marketing collateral. She developed course outlines and training materials for DATASYS4 and third party applications. Ms. Pollack conducted on-site training. She tested applications modules and verified that functional requirements were satisfied.

2.1.3 Technical Teams

2.1.3.1 Subject Matter Experts

Name:	**Shaw, William T. IV**	**Company:**	**MAR**
Labor Category:	**Subject Matter Expert (Master)**	**Employment Status:**	**Employee**
NRC Badge:	(b)(6)	**Country of Citizenship:**	**USA**
Additional Clearance (s):			

Candidates Skills/Experience Relevant to Statement of Work

SOW #	SOW Description	Candidate Qualified
8.1	Project Management	
8.2	Special Projects	✓
8.3	System Authorization	
8.4	Continuous Monitoring Support	
8.5	Data Calls	
8.6	Cyber Situational Awareness	✓
8.7	Policy, Standards and Training	✓

Summary of Skills, Experience, and Training/Certifications Relevant to Statement of Work

Mr. Shaw possesses over 30 years of professional experience as a senior contributor and manager in several organizations involved in computer systems, software design and implementation. Mr. Shaw has specific experience with industrial automation applications. Additionally, Mr. Shaw has extensive Cyber Security technical knowledge and experience and is a Certified Information Systems Security Professional (CISSP). Mr. Shaw is the author of two books, as well as a contributing editor to several others and has published numerous papers and articles. Mr. Shaw is a SME to the ISA on a range of topics, including automation System Cyber Security, and he regularly teaches courses for that organization. Mr. Shaw is a member of the ISA's SP-88, SP-99 and SP-100 committees. In his spare time Mr. Shaw is a contributing editor for security issues to Electric Energy T&D on-line magazine.

Mr. Shaw's education, certifications and Cyber Security experience exceeds the minimum qualifications for the SME (Master) GSA Alliant Small Business labor category.

Mr. Shaw's current experience on the CISSS contract writing policy, developing Cyber Security, inspection procedures, creating course material for inspection personnel, etc. meets/exceeds the requirements of SOW task areas 8.2, 8.6 and 8.7. In his role as a seasoned security professional with regulatory expertise and policy, Mr. Shaw brings SME experience specifically related to policy, standards and training.

Education, Certifications, and Training

Education

- M.S., Engineering Science, Loyola University in Baltimore, (b)(6)
- B.S., Electrical and Computer Engineering, University of Michigan (b)(6)

Certifications and Training

- CAP – Certified Automation Professional
- CISSP – Certified Information Systems Security Professional

Name:	Shaw, William T. IV	Company:	MAR
Labor Category:	Subject Matter Expert (Master)	Employment Status:	Employee

Related Experience: Professional Career Experience

MAR, Incorporated **2010 – Present (2 years)**
Cyber Security Architect

As Cyber Security Architect under the Consolidated Information System Security Services (CISSS) contract, Mr. Shaw participates in the final changes and editing of RG 5.71. He participates in the final changes of NEI 08_09 (rev 6). Mr. Shaw participates in licensee CSP evaluation and RAI generation. He provides a series of technical lunch-hour seminars on computer, networking and Cyber Security topics. He has experience developing the initial Cyber Security Inspection Procedure for licensee CSPs. He has completed an advanced Cyber Security training course at INL. He has experience editing and reformatting a NUREG to explain the technical/security basis of the security controls in the RG 5.71 appendices. Mr. Shaw provides support and Cyber Security training assistance and course material for inspection personnel as part of a course held at INEL. Lastly, he provides as-needed support to NSR personnel on Cyber Security issues.

Securion **2009 – 2010 (1 year)**
Senior Security Analyst

As a Senior Security Analyst, Mr. Shaw performed NERC CIP security assessment for electric utilities and small network penetration testing for electric utilities. He provided consulting services to aid utilities in addressing the NERC CIP requirements. He provided Cyber Security training courses to utility personnel and management. Mr. Shaw generated gap analysis and non-compliance reports regarding CIP conformance and general annual security assessment reports for utility clients. Mr. Shaw was responsible for meeting with client personnel, information gathering and analysis, report generation and formal client presentation of findings. Lastly, he was responsible for year-to-year review of changes in the client security programs and continued compliance with regulations.

Swantech **September 1998 – December 2005 (7 years)**
Chief Technology Officer

As a Chief Technology Officer, Mr. Shaw redesigned the company's condition monitoring product portfolio. He lead an R&D team in designing and developing a PCI based vibration monitoring unit. He lead an R&D team in porting the application onto an embedded Linux platform. Mr. Shaw developed a set of semi-automated vibration analysis tools and utilities to identify gear box issues, drive shaft balance issues and bearing defects. He developed a web-based product offering for the wind-farm market that provided high-level condition assessment and analysis. He developed a cell phone/PDA/Blackberry presentation mechanism for wind farm condition monitoring. Mr. Shaw integrated WiMAX and WiFi mesh networking capabilities into the product design. He redesigned the product offerings for the cruise-ship industry to include spread spectrum wireless communications and Internet connectivity. He was responsible for maintaining and supporting the company web site, email system and servers as well as for the development systems and company laptop PCs. Lastly, he was responsible for managing, hiring and firing technical staff and development personnel.

Cyber Security Consulting **2005 -2007 (2 years)**
Principle

As a Principle, Mr. Shaw provided technical training courses on basic telecommunications, networking, database administration, project management, C/C++ programming, basic SCADA technology, basic DCS technology and basic instrumentation and control concepts. He provided Cyber Security consulting to pipeline operators and electric generating utilities. He developed in-house Cyber Security awareness programs for several companies. He published a book on Cyber Security for SCADA systems and taught courses on industrial automation Cyber Security for the ISA. He published a report for PennWell's pipeline energy sector customers on Cyber Security for Pipeline SCADA Systems. Lastly, he reviewed and developed client policies and procedures and advised on needed changes to meet various regulations such as SOX, HIPPA and the NERC CIPs.

Name:	Shaw, William T. IV	Company:	MAR
Labor Category:	Subject Matter Expert (Master)	Employment Status:	Employee

Tate Integrated Systems **1990 – 2004 (14 years)**
President

As President of Tate Integrated Systems, Mr. Shaw led a team in taking a CREDA software release of a data acquisition system from Los Alamos National Lab and creating an integrated SCADA and DCS product offering. He developed a high-security SCADA system for the California, New England and New York ISOs that allowed real-time, VPN-secured, monitoring and control of generating assets using public networks, including the Internet. He developed a substation automation product that included drivers for a wide range of IEDs and included the ability to extract settings, fault records and oscillographic data from protective relays and stored that data into a web-enabled relational database. Mr. Shaw developed a highly automated storage terminal/tank farm automation system for naval-base and refinery applications. He developed a set of advanced control modules and algorithms for water treatment process plant automation and float-glass production automation. He developed a hybrid RTU product based on Modicon PLC hardware that included integral emergency safety-shutdown capability. Mr. Shaw developed and installed one of the largest and most completely automated water treatment and pipeline delivery system automation projects in North America, combining both DCS and SCADA functionality and did a hot-switch over from the prior system without requiring plant operational interruptions. He recruited, assembled and managed a team of senior staff personnel who were responsible for manufacturing, sales, marketing, HR, accounting, legal and other company departments. Lastly, he was responsible to the board of directors for financial performance, budgets, profitability and growth target.

EMC Systems **1984 - 1989 (5 years)**
President

As President of EMC Systems, Mr. Shaw led the development team for a 3rd-generation SCADA system product that included dual VAX servers, dual Ethernet LAN, X86 based redundant front-end processors and full graphic operator workstations. He developed an advanced family of smart RTUs that included regulatory control and sequential control and calculation capabilities. He developed a set of pipeline-industry applications including batch tracking, line pack, leak detection and meter-run switching plus a full set of RTU-based volumetric calculations including AGA-3,5,7 and NX-19. He installed and commissioned one of the largest product pipeline SCADA systems in North America. Mr. Shaw developed a library of serial protocols drivers for the entire legacy SCADA vendor RTUs and for existing competitor's RTU products. He recruited, assembled and managed a team of senior staff personnel who were responsible for manufacturing, sales, marketing, HR, accounting, legal and other company departments. Lastly he was responsible to the board of directors for financial performance, budgets, profitability and growth targets.

EMC Controls **1980 – 1984 (4 years)**
V.P. of Engineering

As V.P. of Engineering at EMC Controls, Mr. Shaw started a Project and Contract Management Department to handle large I&C automation projects both domestically and internationally. He led the development team for a 2nd-generation DCS product (the D/3) that included a dual, high-speed token ring LAN and X86 based redundant controllers and operator workstations. He developed an advanced BATCH object-oriented process control package and language. He was the keynote speaker and principle member of the ISA's SP-88 committee on batch automation standards. Mr. Shaw was awarded the Valor award (Chemical Engineering magazine) for advancement of plant and process automation due to the D/3 process control system. He was awarded the year's best automation article by Control Engineering magazine. He led the creation and management of a manufacturing and test department and production organization. He supervised over 110 professional engineers and middle-managers and over $65M in project activity annually. Lastly, he published Computer Control of BATCH Processes.

Name:	**Shinn, Michael T.**	**Company:**	**Prometheus Global**
Labor Category:	**Subject Matter Expert (Master)**	**Employment Status:**	**Employee**
NRC Badge:	(b)(6)	**Country of Citizenship:**	**USA**
Additional Clearance (s):			

Candidates Skills/Experience Relevant to Statement of Work

SOW #	SOW Description	Candidate Qualified
8.1	Project Management	
8.2	Special Projects	✓
8.3	System Authorization	✓
8.4	Continuous Monitoring Support	✓
8.5	Data Calls	
8.6	Cyber Situational Awareness	✓
8.7	Policy, Standards and Training	✓

Summary of Skills, Experience, and Training/Certifications Relevant to Statement of Work

Mr. Shinn has over 20 years of professional experience in the Cyber Security field, and has been the co-founder of a number of security companies where he has worked with numerous Federal Agencies and Fortune 500 companies. He has co-authored the following: Regulatory Guide 5.71, Cyber Security Programs for Nuclear Facilities; Other NRC Regulatory Guides and NUREGs; and Troubleshooting Linux Firewalls, published by Addison Wesley Professional. He is a founder of Atomicorp, a virtualization and cloud security products firm, and was a key member of the original Wheelgroup Corporation, developers of the first major intrusion detection system and pioneers of penetration testing.

Mr. Shinn is considered an expert in Cyber Security having obtained multiple certifications and over 20 years of information systems experience. His senior level experience exceeds the minimum qualifications of the SME (Master) GSA Alliant Labor Category. Mr. Shinn is a member of the Advisory Board at the SANS Institute, and is an invited speaker at numerous security events held by organizations such as the University of Maryland, SANS, the State of Colorado, CSI and others. He is also an Association of Computing Machinery (ACM) instructor, and was a founding member of the George Mason University Security Review Panel in 1995 which developed the University's security policies, adjudication process, and managed the University's Computer Emergency Response Team (CERT).

Mr. Shinn has provided SME level security, privacy, regulatory and program management support for various government agencies in the field of Cyber Security, which qualifies him to provide SME support in the SOW areas 8.2, 8.3, 8.4, 8.6, and 8.7. Mr. Shinn's current experience working on the CISSS contract includes Chief Certifier, Instructor for NRC Cyber Security Training, Investigations regarding regulatory violations and has provided feedback on proposed rules related to regulatory requirements. In addition, he has developed policy and procedures to support the Cyber Security Office (CSO), led certification teams, supported the technical review board and developed segment architectures as directed by CSO.

Education, Certifications, and Training

Education

- B.S., Economics, George Mason University, (b)(6)

Certifications and Training

- Information Assurance Security Officer (IASO)
- Facility Security Officer (FSO)
- NRC Site Access Authorization Training, March 2012
- NRC Fuel Cycle F-201, 2011
- NRC Reactor Fundamentals

Name:	Shinn, Michael T.	Company:	Prometheus Global
Labor Category:	Subject Matter Expert (Master)	Employment Status:	Employee

Related Experience: Professional Career Experience

Prometheus Global **September 2002 to Present (9.8 years)**

CEO, Security and Privacy Expert

Mr. Shinn is the CEO for Prometheus Global, providing security, privacy and regulatory support as well as program management support for its clients.

Selected Projects and Customers include:

Nuclear Regulatory Commission (NRC)

- Testified numerous times before ACRS and NRC Commissioners on Cyber Security and Licensee topics.
- Works closely with NSIR, NMSS and other program offices on Cyber Security issues.
- Currently working with NMSS and NSIR on Reactor and Fuel Cycle Cyber Security issues, including development of road map/path forward recommendations, draft rule making, guidance development and licensee interactions.
- Co-authored RG 5.71 (Cyber Security Programs for Nuclear Facilities).
- Co-authored changes to Appendix G, 10 CFR 73.
- Co-authored changes to RG 5.69 (Design Basis Threat).
- Co-authored changes to DG 5019 for Cyber Security report-ability rule changes.
- Working on behalf of NRC to determine enforceability of NEI documents to include 08-09, 10-04, white papers, feedback on proposed rules and to solicit changes that would meet regulatory requirements.
- Provided SME level support for CSP review teams on regulatory and cyber issues.
- Support and participate in investigations regarding regulatory violations and allegations by licensees and licensee personnel, and participate in Regulatory Conferences on behalf of NRC for licensee violations of regulations.
- Support NSIR in investigations of sensitive national security matters involving licensees and other federal agencies.
- Chief certifier for systems in support of Cyber Security Office, such as MPKI, IPSS, NSTS and others.
- Instructor for NRC Cyber Security training, including Executive, Management and Staff level training, as well as specialized training for program offices to include NSIR and NMSS licensee focused Cyber Security training.
- Provide SME level support to CSO on various tasks to include development of policy and procedures, lead certification teams, support technical review board, and develop segment architectures and other SME tasks as directed by CSO.

Department of Defense – US Army Intelligence and Security Command (INSCOM)

- Project Manager and SME for multiple classified IC Cyber Security programs.

Department of Defense – Inspector General (DoDIG)

- Manager of Attack and Penetration (A&P) team for a classified DoDIG auditing effort of an internal DoD agency.

Office of Management and Budget (OMB)

- Performed federal government wide assessment of FDCC compliance for all score card agencies, development of policy, and assessment of roadmap and develop whitepapers to help OMB set federal government direction. Assessed agencies included DOD, Commerce, Education, EPA, HHS, VA, DHS, HUD, DOT, GSA, NSF, OPM, SBA, State, Justice, Treasury, DOI, DOL, DOE, NASA, Social Security and others.

Name:	Shinn, Michael T.	Company:	Prometheus Global
Labor Category:	Subject Matter Expert (Master)	Employment Status:	Employee

USDA

- Worked directly with CIO and Deputy CIO to develop turnaround plan for improved FISMA compliance.

Department of Labor (DoL)

- Managing team and providing primary support to Chief Architect for Department of Labor in aid of Security, Privacy and Enterprise Architecture Technical and Policy decision making and support in aid of DOL wide IT strategy. Served as co-chair of DOL IT Architecture Sub-Committee and DOL IPv6 task force. Also DOL representative for the Federal Government IPv6 Working Group and Federal CIO Council, and member of Federal IPv6 Security Sub-Committee. Also served as facilitator for the DoL Technology Standards Review Board and the UDTI.

Federal Trade Commission

- Lead for Certification team for FTC's Do-Not-Call system.

Federal Reserve

- Managed effort to audit security and financial controls of Federal Reserve, and to conduct penetration test and gap analysis of Cyber Security controls.

United Nations

- Led forensics engagement for the UN. Details sensitive and undisclosed.

General Services Administration (GSA)

- Provided security and engineering consulting services, including host audits, remediation, Independent Verification and Validation (IV & V) and Certification and Accreditation (C & A) efforts for the GSA schedule systems.

Veterans Hospital Administration (VHA)

- Team Leader for the Veterans Hospital Administration Security Certification and Accreditation team, performing on-site security evaluations at Veterans Hospitals worldwide in aid of the agency's NIST 800-53 compliance efforts. This effort was the first of its kind undertaken by the Federal Government under FISMA requirements.

Secure Software, Inc. (subsidiary company, acquired by Fortify) **March 2001 - August 2002 (1.4 years)**
CEO and Founder

Secure Software's focus was on helping companies make their products, hardware and software more secure and reliable in an economically feasible, scalable and repeatable manner. Secure Software's customers included the US Navy, US Air Force, DARPA, The Federal Reserve, Corbett Technologies (now BAE), DigiMark and other government and commercial organizations.

The Shadow Group, Inc. **September 2000 – April 2001 (8 months)**
(acquired by Corbett Technologies in 2001)
Partner and Founder

The Shadow Group was a full services information assurance and risk management firm. Customers included UUNet/MCI WorldCom, BBO, The White House (Executive Office of the President) and other commercial and Government entities.

Mr. Shinn developed and led the Shadow Group's Product Security Posture Assessment (PSPA) offering that evaluated the security state of third party products purchased or evaluated by client companies, such as control/safety devices, IA technologies and other high risk technologies. This gave the Shadow Group's clients a trusted third party evaluation of the security posture of vendor products, as well as how

Name:	Shinn, Michael T.	Company:	Prometheus Global
Labor Category:	Subject Matter Expert (Master)	Employment Status:	Employee

the products conformed to that organization's risk management and compliance policies. The assessment ranged from design analysis to full hardware reverse engineering and in-depth technical code audits of various products.

Mr. Shinn also co-managed and led a team that operated a classified computer forensics lab in support of the National Archives (NARA) and the White House. The purpose of the lab was data recovery of degraded, damaged and otherwise compromised magnetic media from the Clinton administration. The data was needed to provide documentation and discovery in a legal action against the United States Government. Mr. Shinn served as SME, ISSO and Risk Manager for the length of the contract.

Plesk, Inc. **July 1999 to September 2004 (5.2 years)**
(acquired by SW-Soft, now Parallels, in September 2004)
Board of Director and Co-Founder

Plesk, Inc. was a software company which designed virtualization and automation solutions for enterprises and service providers. Mr. Shinn provided director level oversight of the company's strategy, risk management and operations and assisted the management team in determining the technology direction for the company.

Cisco Systems, Inc. **August 1998 - July 1999 (1 year)**
Senior Software Developer/Research Scientist

Mr. Shinn was a developer on the Netranger Intrusion Detection product and the Netsonar Vulnerability Assessment product. He also wrote new exploits to find security vulnerabilities in all manner of OSes as part of the NetSonar product and developed new methods for defending systems and networks against attack.

Wheelgroup Corporation **August 1997 - August 1998 (1 year)**
(acquired by Cisco Systems, August 1998)
Senior Network Security Engineer/Auditor

Mr. Shinn led teams conducting Security Posture Assessments and Security Design Reviews for customers. This included performing security audits on the largest corporations in the world, comprising all known operating systems, network devices, DCS/SCADA/Safety systems/devices and other networked technologies. He also conducted ongoing research into security of Control systems and devices, Operating Systems, Networks, Applications and other concepts, such as designing trusted models, exploitation tools, vulnerabilities, counter measures, re-scaling models to fit threat, etc. Developed automated framework for conducting control and safety system tests of production systems.

Mr. Shinn was responsible for the development of Wheelgroup's automated Security Posture Assessment/penetration testing tools, modules, scripts and engines (AUTOSPA). He also designed Intrusion Detection deployment strategies for customers using Wheelgroup's Netranger product and helped test the product with live networks at customer sites.

United States Securities and Exchange Commission **August 1996 – August 1997 (1 year)**
Project Leader/Systems Engineer

He was responsible for developing, engineering and managing the security requirements development, policy creation and operational implementation of the SEC EDGAR internet systems and making security recommendations to other divisions and the SEC management for the EDGAR internet project.

Name:	Shinn, Michael T.	Company:	Prometheus Global
Labor Category:	Subject Matter Expert (Master)	Employment Status:	Employee

Executive Office of the President, The White House — **June 1995 – June 1996 (1 year)**
Computer Analyst

Mr. Shinn was a member of a systems administration team responsible for all White House Internet-connected machines, including boundary control devices. He worked with the Secret Service to investigate electronic threats against White House personnel, such as e-mail threats against the POTUS and other high profile officials and also was responsible for investigating all attacks against White House systems and acting as primary point of contact with outside organizations and agencies for case development.

KTI, Inc. — **January 1992 – June 1995 (3.5 years)**
Computer Analyst

Mr. Shinn was responsible for managing the company's servers and workstations. He was also responsible for the security of all systems, as well as developing new data management solutions for global operations and was responsible for leading the company's transition from token ring to ethernet.

Name:	**Kragen, Scott**	**Company:**	**KCG**
Labor Category:	**Subject Matter Expert (Senior)**	**Employment Status:**	**Employee**
NRC Badge:	(b)(6)	**Country of Citizenship:**	**USA**
Additional Clearance (s):			

Candidates Skills/Experience Relevant to Statement of Work

SOW #	SOW Description	Candidate Qualified
8.1	Project Management	
8.2	Special Projects	✓
8.3	System Authorization	✓
8.4	Continuous Monitoring Support	✓
8.5	Data Calls	
8.6	Cyber Situational Awareness	✓
8.7	Policy, Standards and Training	

Summary of Skills, Experience, and Training/Certifications Relevant to Statement of Work

Scott Kragen is a technical Cyber Security professional with more than 13 years of experience in conducting vulnerability assessment, penetration testing and incident response across Federal Agencies such as the FBI, Department of Treasury, Office of Personnel Management and many others. Mr. Kragen has an in-depth knowledge of NIST requirements and conducting exploitation operations in support of Security Test & Evaluation assessments in accordance with Federal standards.

Mr. Kragen has over 13 years of IT experience with a strong background in Cyber Security, which exceeds the requirements related to the Subject Matter Expert (Senior) GSA Alliant Small Business Labor Category. In addition, Mr. Kragen's certifications as an Expert Penetration Tester, Ethical Hacker, CISSP, Offensive Security Wireless Professional, Mile2 Certified Pen Testing Specialist and Offensive Security Certified Professional along with his Bachelors of Science in IT further certifies him as a SME. Mr. Kragen's technical knowledge in the areas of Security Test & Evaluation and documentation further confirms his extensive knowledge of Cyber Security practices. Lastly, Mr. Kragen has played a key role in drafting policy related to ATO's and major/minor system determination in accordance with NIST standards.

Mr. Kragen's experience exceeds the duties required under SOW areas 8.2, 8.3, 8.4 and 8.6 for this position. As a Senior Security Engineer & Lead Penetration Tester, Mr. Kragen plans, documents, schedules and executes (where appropriate, with the assistance of Security Engineers) the ST&E assessments, to include technical testing, interviews, and observations. He regularly utilizes automated technical testing tools, to include AppDetective, Nessus, and WebInspect. He reviews the reports from the technical testing to determine system vulnerabilities, documents the identified vulnerabilities with deficiencies in the security controls mandated by NIST SP 800-53, and generates POA&Ms. He documents system vulnerabilities within the system Security Assessment Report and Risk Assessment to provide the CISO and Designated Approval Authority (DAA) with the level of risk system vulnerabilities pose to the agency. Mr. Kragen drafts associated C&A package memos from the CISO to the DAA and from the DAA to the SO making recommendations regarding the Authority to Operate. He reviews, processes and recommends either approval or denial for numerous waiver and exception requests involving 10 operational systems for which he is responsible. He participates in the Change/Configuration Control Board (CCB) process to include reviewing Request for Change for assigned systems and documenting the implications of approval/denial to the government client's CCB voting member. Mr. Kragen assures appropriate application of controls over unauthorized data reuse, facilitating the decommissioning of laptops and the subsequent physical destruction of over 50 hard drives. He works with agency Managed Service Provider to develop a secure baseline for the Solaris 10 Operating System (OS) Lastly, he works with SOs of two Major Applications to convert them to Minor Applications, and also the SOs of the General Support Systems that were taking on the Minor Applications.

Name:	Kragen, Scott	Company:	KCG
Labor Category:	Subject Matter Expert (Senior)	Employment Status:	Employee

Education, Certifications, and Training

Education

- BS, Information Technology – Rochester Institute of Technology, (b)(6)

Certifications and Training

- GIAC Certified Web Application Penetration Tester
- Certified Expert Penetration Tester
- Certified Penetration Tester
- Certified Ethical Hacker
- CISSP
- Offensive Security Wireless Professional
- Mile2 Certified Pen Testing Specialist
- Offensive Security Certified Professional

Related Experience: Professional Career Experience

Knowledge Consulting Group, Inc. **January 2011 – Present (1.3 years)**

Senior Security Engineer and Lead Penetration Tester

As the Senior Security Engineer and Lead Penetration Tester, Mr. Kragen is responsible for the following duties:

- Plan, document, schedule and execute (where appropriate, with the assistance of Security Engineers) the Security Test and Evaluation (ST&E) assessments, to include technical testing, interviews, and observations.
- Review the reports from the technical testing to determine system vulnerabilities, document the identified vulnerabilities with deficiencies in the security controls mandated by NIST SP 800-53, and generating POA&Ms.
- Document system vulnerabilities within the system Security Assessment Report and Risk Assessment to provide the CISO and Designated Approval Authority (DAA) with the level of risk system vulnerabilities pose to the agency.
- Draft associated C&A package memos from the CISO to the DAA and from the DAA to the SO making recommendations regarding the Authority to Operate.
- Review, process and recommend either approval or denial for numerous waiver and exception requests involving 10 operational systems for which he is responsible.
- Participate in the Change/Configuration Control Board (CCB) process to include reviewing Request for Change for assigned systems and documenting the implications of approval/denial to the government client's CCB voting member.
- Assure appropriate application of controls over unauthorized data reuse, facilitating the decommissioning of laptops and the subsequent physical destruction of over 50 hard drives.
- Work with agency Managed Service Provider to develop a secure baseline for the Solaris 10 Operating System (OS).
- Work with SOs of two Major Applications to convert them to Minor Applications, and also the SOs of the General Support Systems that were taking on the Minor Applications.
- Work on numerous ad hoc projects to include: created standardized SAR and RA language related to agency (RTM) and NIST SP 800-53 controls; wrote decision memos to assist in determining if a system would be considered a Major/Minor Application; working with a team to improve the RMS tool; and assisted with updating, and creation of Standard Operating Procedures relating to the four phases of C&A (as defined by NIST SP 800-37) and the POA&M process.

Fannie Mae **February 2010 – January 2011 (11 months)**

Senior Security Engineer

As Senior Security Engineer Mr. Kragen performed the following duties:

- Lead vulnerability assessment engineer for a network of 10k+ servers and 12k workstations.
- Developed the standards and procedures for performing vulnerability assessment for the corporation based on current industry methods.

Name:	Kragen, Scott	Company:	KCG
Labor Category:	Subject Matter Expert (Senior)	Employment Status:	Employee

- Introduced new procedures for evaluating software ports and services and risks it might introduce to the network.
- Acted as first response in incidents and was on call once a month for a week rotation.
- Provided guidance and training for the junior support staff on the team.
- Acted as consultant to the company for many projects involving deployed future projects.
- Researched new security technologies.

Northrop Grumman **April 2008 – February 2010 (1.8 years)**
Senior Security Engineer

As Senior Security Engineer was responsible for the following:

- Lead vulnerability assessment engineer supporting DHS on a closed network.
- Performed security testing and evaluation on all applications and systems based on DISA STIGS.
- Executed application security testing based upon DISA STIGS and OWASP guidelines.
- Acted as first response in incidents and worked regularly with security operation center.
- Helped in the cleanup of classified spillages.
- Worked directly with the engineers of the network operation center to close vulnerabilities and offer advice for mitigations.
- Supported external auditors in the assessment of our network for re-certification.

Booz Allen Hamilton **November 2007 – April 2008 (5 months)**
Senior Consultant

As a Senior Consultant performed the following:

- Supported the operation and maintenance of the full service directory and white pages for the Defense Intelligence Agency.
- Worked with LDAP servers updating and maintaining the schema for GAL syncs and Live Syncs through tools such as ADAM, MIIS, and DSACLS.
- Toubleshoot PKI issues and assist users in obtaining user certifications as a trusted agent.

Harris Corporation **November 2005 – November 2007 (2 years)**
Senior Systems Administrator II

As Senior Systems Administrator II Mr. Kragen was responsible for the following duties:

- Support to the Commanding Officers office at the Navy Research Lab. Supported 150 machines with a mixed environment of Windows XP, 2003 Server, and OS X.
- Developed and implemented single sign on for both the OS X and Windows users.
- Involved in the sanitation of several exchange servers, backups and backup servers, and workstations during several spillage incidents.
- Maintained multiple platform server systems. Managed multiple Exchange servers. Performed and maintained daily backups and support for users.
- Maintained and performed security evaluations of workstations.

Name:	Kragen, Scott	Company:	KCG
Labor Category:	Subject Matter Expert (Senior)	Employment Status:	Employee

Harris Orkand Information Systems — **May 2003 – November 2005 (2.5 years)**
Senior Systems Analyst II

As the Senior Systems Analyst II, Mr. Kragen performed the following responsibilities:
- Deployed Windows 2000/XP and Oracle systems at State Department Posts worldwide.
- Served as technical lead providing support during systems installations and onsite training for staff on the consular applications of the State Department.
- Trained Foreign Service officers in fingerprint gathering of non-immigration visa applicants.

Thunderwave, Inc. / Beyondguide, Inc. — **July 1999 – January 2002 (2.6 years)**
Systems Engineer / Sound Technician

As the Systems Engineer / Sound Technician responsible for the following:
- Maintained five server systems and two Checkpoint firewalls with VPN connectivity.
- Configured Exchange 5.5, NT 4.0, Oracle, Tomcat/Apache, Lotus QuickPlace and Linux.
- Directly supported all data backup/recovery, virus protection, system security, new technology research, new server/workstation builds and related projects for a staff of 50.

Rochester Institute of Technology — **1998 – 1999 (1 year)**
Macintosh / PC Support Specialist

As the Macintosh / PC Support Specialist performed the following duties:
- Installed, configured, upgraded and maintained operating systems and 3rd party applications.
- Troubleshot emerging problems across both Macintosh and Windows platforms.
- As Network Specialist installed, troubleshot and maintained Windows and Mac operating systems and applications.
- Administered NT network, resolved problems with routers, switches and other devices.

2.1.3.2 Information Assurance/Security Specialists

Name:	**Tharp, Benjamin**	**Company:**	**Prometheus Global**
Labor Category:	**Information Assurance/Security Specialist (Master)**	**Employment Status:**	**Employee**
NRC Badge:	(b)(6)	**Country of Citizenship:**	**USA**
Additional Clearance (s):			

Candidates Skills/Experience Relevant to Statement of Work

SOW #	SOW Description	Candidate Qualified
8.1	Project Management	
8.2	Special Projects	✓
8.3	System Authorization	✓
8.4	Continuous Monitoring Support	✓
8.5	Data Calls	
8.6	Cyber Situational Awareness	✓
8.7	Policy, Standards and Training	

Summary of Skills, Experience, and Training/Certifications Relevant to Statement of Work

Benjamin Tharp has over seven years of professional experience in the field of Information Systems/Information Technology, with 4.6 of those years concentrated in Information Systems Security. Mr. Tharp has provided engineering and systems expertise to both individual and corporate clients. He has spent over the last four years specializing in end user technologies, with a focus on Information Assurance, Certification and Accreditation and non-repudiation of systems data.

Mr. Tharp's current experience working on the CISSS contract meets the minimum qualifications for the Information Assurance/Security Specialist (Master) GSA Alliant Small Business Labor Category. In his role as a Senior Security Analyst, Mr. Tharp acts as the Information System Security Officer (ISSO) for two systems with responsibilities for creating, updating, reviewing security documentation, developing system security plans and contingency plans. He is also responsible for completing and monitoring POA&M's for each system. Mr. Tharp acts as the lead assessor for numerous systems certifications and authorizations which includes performing ST&E, Security Risk Assessments (SRA) and Vulnerability Assessments.

Mr. Tharp has over three years of experience working with NRC systems in support of special projects, authorization efforts, system documentation updates, and continuous monitoring support which exceeds the requirements set forth in SOW areas 8.2, 8.3, 8.4 and 8.6. Mr. Tharp has performed C&A for over 10 NRC systems, which includes ST&E reports, SRA, Vulnerability Assessment reports, and POA&M's. Mr. Tharp has performed over 10 Annual Security Control Tests, along with quarterly scans of multiple systems. He has updated contingency plans and developed contingency plan test reports, and provides updates to the SRA and SSP. Mr. Tharp has experience in facilitating incident response efforts. In addition, he has assisted in developing procedures in incident handling which include incident response training of system personnel on incident handling. He has experience with handling, monitoring and reporting incident responses and provided incident response reports and lessons learned.

Education, Certifications, and Training

Education

- Graduate, (b)(6)

Certifications and Training

- MCP (Windows 2000), 2004
- Information Assurance Security Officer (IASO), 2008
- Information Technology Infrastructure Library (ITIL), 2012
- Certified Ethical Hacker (CEH) Training
- Certified Information Systems Security Professional (CISSP) Training

Name:	Tharp, Benjamin	Company:	Prometheus Global
Labor Category:	Information Assurance/Security Specialist (Master)	Employment Status:	Employee

Related Experience: Professional Career Experience

Prometheus Global, Inc. **November 2007 – Present (4.6 years)**

Senior Security Analyst

Mr. Tharp acts as the ISSO for two systems within the NRC with responsibilities including creation/updating/reviewing of system security documentation such as SSPs and Contingency Planning documentation. He is also responsible for completing/monitoring/updating the associated POA&M's for each system as well as various ISSO related day-to-day functions.

He acts as Lead Assessor for numerous system certifications and authorizations within the NRC which includes performing ST&Es, SRAs and Vulnerability Assessments, as well as creating/updating supporting documentation such as SSPs, Security Categorizations, Operational Procedure Guides, and POA&Ms.

He has performed and reviewed vulnerability scans and authored reports and recommendations for the Institute of Defense Analyses (IDA) to assist in their efforts of ongoing security. Mr. Tharp authored various documents including SSP, Residual Risk Reports (RRR), and RA in aid of the National Indian Gaming Commission's FISMA compliance efforts.

Mr. Tharp is a member of the Environmental Protection Agency Security Certification and Accreditation Team, conducting both on and off-site interviews and authoring a SSP and a RA in aid of the agency's NIST 800-53 and FISMA compliance efforts.

He provided systems engineering services for International consulting firm The Services Group as well as IT support for a staff of 50-70 end users both on-site and remote which included purchasing equipment, scheduled maintenance and server/workstation support.

Self Employed **October 2006 – November 2007 (1.1 years)**

IT Consultant Technician

Mr. Tharp installed a music computer library and established the foundation for the network infrastructure (cabling, router configuration, building serves and workstation and construction) for a Point of Sales (POS) system in local family fun center.

He also spec/built computers based on clients needs, provided technical support, installation of antivirus programs, scrubbed systems of malware, performed software and hardware upgrades, established wireless networks, printer configuration, established back up routines.

CompUSA **March 2005 – October 2006 (1.6 years)**

Technical Services Sales Manager

Mr. Tharp served as the Manager of the Technical Services Sales Department where he was responsible for managing technicians, inventory management, financial management and budgeting, ensuring the work was done properly, customer contact and feedback, technician schedules. He also acted as a technician. He provided technical dynastic and troubleshooting activities on PC/Mac desktops, laptops and printers. He also performed PC/Mac desktop and laptop repairs, installations and upgrades. In his last six months Mr. Tharp managed the tech shop as well as the store manager in CompUSA Fairfax store.

Name:	**Wijetunga, Suneth**	**Company:**	**MAR**
Labor Category:	**Information Assurance/Security Specialist (Master)**	**Employment Status:**	**Contingent Hire Employee**
NRC Badge:	(b)(6)	**Country of Citizenship:**	**USA**
Additional Clearance (s):			

Candidates Skills/Experience Relevant to Statement of Work

SOW #	SOW Description	Candidate Qualified
8.1	Project Management	
8.2	Special Projects	✓
8.3	System Authorization	✓
8.4	Continuous Monitoring Support	✓
8.5	Data Calls	
8.6	Cyber Situational Awareness	✓
8.7	Policy, Standards and Training	✓

Summary of Skills, Experience, and Training/Certifications Relevant to Statement of Work

Suneth Wijetunga possesses over 12 years of professional experience in enterprise IT security initiatives including planning, analysis and implementing solutions in support of business objectives. Extensive involvement in compliance and IT audits based on NIST publications, FISMA, and OMB directives for the Federal Government. He has special skills in technology driven process re-engineering initiatives to achieve business objectives of higher productivity, reduction in cost, improvement in quality and service levels. Technical skills in the development and implementation of electronic commerce applications. Proficiency in web usability guidelines and their application in designing effective web sites. Possesses extensive knowledge in database design and management. Broad technical and analytical skills and business experience in implementation of web integration projects with various back-end database systems. Mr. Wijetunga has extensive experience in Nessus, CORE Impact and other vulnerability scanning tools.

Mr. Wijetunga's 12 years of information security experience exceeds the minimum qualifications of the Information Assurance/Security Specialist (Master) GSA Alliant labor category. He currently has hands on experience working on the NRC CISSS contract as a Lead Security Analyst. His duties and responsibilities include supporting NRC offices on IT security matters and providing guidance on remedying security deficiencies, developing security documentation in support of authorization of systems, leading security assessments such as ST&Es in support of authorization of NRC IT systems, and acting as one of two certifying agents for NRC IT systems in support of ATO. Mr. Wijetunga leads and manages FISMA assessment efforts at NRC to ensure compliance with the NIST and other agency specific requirements, and heads continuous monitoring efforts at NRC offices that meet federally mandated and NRC defined security requirements.

In his role as Lead Security Analyst on the CISSS contract, Mr. Wijetunga currently fulfills the SOW areas of 8.2, 8.3, 8.4, 8.6 and 8.7 as follows: on 8.2 he supports NRC offices on IT security and provides guidance on remedying deficiencies and minimizing risks. On 8.3 he is one of two certifying agents in support of ATO. He leads security assessments such as ST&E and he leads and manages FISMA assessments to ensure compliance with NIST. On 8.4 Mr. Wijetunga leads continuous monitoring efforts at NRC offices that meet federally mandated and NRC defined security requirements, including resolution and quarterly reporting of POA&M. He also provides annual support of contingency planning, updating of security documentation, annual security controls testing, quarterly system scanning and reporting and providing security engineering support to verify and validate IT system architectures and implementations. On 8.6, Mr. Wijetunga also manages vulnerability scanning and penetration testing engagements and on 8.7 he develops security standards documentation for NRC.

Mr. Wijetunga has signed a letter of intent to become a MAR employee upon award of CSPSS.

Name:	Wijetunga, Suneth	Company:	MAR
Labor Category:	Information Assurance/Security Specialist (Master)	Employment Status:	Contingent Hire Employee

Education, Certifications, and Training

Education

- B.S., Decision & Information Technology, Cum Laude, University of Maryland, (b)(6)
- B.S., Microbiology, Cum Laude with High Honors, University of Maryland, (b)(6)

Certifications and Training

- Virtualization Security, July 2011
- Commercial Nuclear Power Cybersecurity, May 2011
- ITIL v3 Foundation Certificate, 2011
- CISM – Certified Information Security Manager, 2009
- CISSP – Certified Information Systems Security Professional, 2009
- CISA – Certified Information Systems Auditor, 2008
- Auditing Oracle Databases, November 2007
- Business Continuity Planning, October 2007
- Government Auditing Standards, September 2007
- Audit Risk Management, May 2007
- Auditing Operating Systems, March 2007

Related Experience: Professional Career Experience

Force 3 — **May 2009 – Present (3.1 years)**
Lead Security Analyst

On the CISSS contract supporting the NRC, Mr. Wijetunga serves as the Lead Security Analyst. His duties and responsibilities include supporting NRC offices on IT security matters and providing guidance on remedying security deficiencies, developing security documentation in support of authorization of systems, leading security assessments such as ST&E in support of authorization of NRC IT systems, acting as one of two certifying agents for NRC IT systems in support of ATO. Mr. Wijetunga also leads and manages FISMA assessment efforts at NRC to ensure compliance with the NIST and other agency specific requirements, and heading continuous monitoring efforts at NRC offices that meet federally mandated and NRC defined security requirements including resolution and quarterly reporting of POA&M, annual support of contingency planning, updating of security documentation, annual security controls testing, quarterly system scanning and reporting and providing security engineering support to verify and validate IT system architectures and implementations that are based on sound security engineering principles and practices. Mr. Wijetunga also manages vulnerability scanning and penetration testing engagements and develops security standards documentation for the NRC.

Holloway & Co. PLLC, Wash. D.C. — **January 2007 – April 2009 (2.3 years)**
Senior IT Manager

Overall responsibilities included managing IT audit engagements, project planning, budgeting and writing proposals. He also reviewed and updated IT audit programs to conform to current guidelines. Client specific responsibilities and duties included assisting clients in the development of system security documents; participating in the development or revision of system-specific security safeguards and local operating procedures that are based on federal guidelines; analyzing and assessing customer information systems and networks for conformance with policy and guidelines and evaluating security controls for applicability to requirements and making recommendations on control assignment and methodologies to implement controls.

Christian Service Charities — **October 2004 – January 2007 (2.3 years)**
Technology Manager

Formulated IT strategy and reviewed and analyzed all information technology needs within the organization including management of the Membership database, Pledge Distribution database, organizational web sites and organization wide network, firewall and maintenance.

Name:	Wijetunga, Suneth	Company:	MAR
Labor Category:	Information Assurance/Security Specialist (Master)	Employment Status:	Contingent Hire Employee

Euclid Technology, LLC **January 2001 – October 2004 (3.8 years)**
Software Engineer

Mr. Wijetunga was the Technical Lead/Project Manager for web integration projects including requirements analysis, developing action plans and envisioning solutions that fulfill client expectations. Supported Project Implementation Team to design, develop and test database triggers and procedures that provided customized solutions to meet organizational requirements of clients. Developed, maintained and managed company web site and maintained and managed company network, firewall and client servers.

Name:	**Pham, Brian B.**	**Company:**	**MAR**
Labor Category:	**Information Assurance/Security Specialist (Entry-Level)**	**Employment Status:**	**Employee**
NRC Badge:	(b)(6)	**Country of Citizenship:**	**USA**
Additional Clearance (s):			

Candidates Skills/Experience Relevant to Statement of Work

SOW #	SOW Description	Candidate Qualified
8.1	Project Management	
8.2	Special Projects	✓
8.3	System Authorization	✓
8.4	Continuous Monitoring Support	✓
8.5	Data Calls	
8.6	Cyber Situational Awareness	✓
8.7	Policy, Standards and Training	✓

Summary of Skills, Experience, and Training/Certifications Relevant to Statement of Work

Brian Pham possesses five years experience in the Information Technology field with three years experience in FISMA Information Assurance/IT Security compliance activities. Mr. Pham has multiple years of experience working with computers including hardware, small scale networking, and vulnerability scanning and troubleshooting. Mr. Pham also has four years of administrative experience which has contributed to his efficient and productive working environment.

Mr. Pham's experience exceeds the minimum qualifications of the Information Assurance/Security Specialist (Entry-Level) GSA Alliant Labor Category. As a Technical Writer/Security Specialist under the NRC CISSS contract, Mr. Pham assists in the preparation of C&A artifacts following NIST and NRC standards. He performs security analysis by scanning networks using specialized tools such as Nessus, Hailstorm, DISA Gold Disc, and Core Impact. He conducts security reviews and analysis using DISA, CIS, and NIST STIGs. He has experience using Hailstorm for Web Application testing. He has populated over 40 information systems in ASSERT with current Security Control data. Mr. Pham develops procedural guides for technical procedures such as patching and standard computer configurations. He creates and populates Vulnerability Tracking Sheets, Finding Tracking Sheets, Quarterly Scan Reports and other documentation as a result of Scanning, reviews results with customer for ST&E. He provides analysis of findings and solutions to the customer.

Mr. Pham manages multiple laptops, classified and unclassified, for the Computer Security Office at the NRC. He upgrades computer hardware following federal IT security standards. He hardens servers and computers using hardening standards provided by DISA and NIST. He encrypts computers for security following federal and agency standards. He enters POA&M items for NRC information systems using their designated C&A tools. His current experience working on the CISSS contract qualifies him to support the duties required under SOW 8.2, 8.3, 8.4, 8.5, 8.6 and 8.7 for CSPSS.

Education, Certifications, and Training

Education

- Computer Science Major, Montgomery College, (b)(6)
- Information Systems Management Major, University of Maryland University College

Certifications and Training

- ITIL v3 Foundation Certified, 2011
- Core Impact CICP Certified Professional
- Hailstorm Professional
- NRC System Administrator's Roles & Responsibilities For Protecting Unclassified Systems

Name:	Pham, Brian B.	Company:	MAR
Labor Category:	Information Assurance/Security Specialist (Entry-Level)	Employment Status:	Employee

Related Experience: Professional Career Experience

MAR, Incorporated — **September 2006 – Present (5.8 years)**

Technical Writer/Security Specialist — *October 2008 - Present*

As a Technical Writer/Security Specialist under the CISSS contract, Mr. Pham assists in the preparation of C&A artifacts following NIST and NRC standards. He performs security analysis by scanning networks using specialized tools such as Nessus, Hailstorm, DISA Gold Disc, and Core Impact. He conducts security reviews and analysis using DISA, CIS, and NIST STIGs. He has experience using Hailstorm for Web Application testing. He has populated over 40 information systems in ASSERT with current Security Control data. MR. Pham develops procedural guides for technical procedures such as patching and standard computer configurations. He creates and populates Vulnerability Tracking Sheets, Finding Tracking Sheets, Quarterly Scan Reports and other documentation as a result of Scanning, reviews results with customer for ST&E. He provides analysis of findings and solutions to provide to the customer. He manages multiple laptops, classified and unclassified, for the Computer Security Office at the NRC. He upgrades computer hardware following federal IT security standards. He hardens servers and computers using hardening standards provided by DISA and NIST. He enters POA&M items for NRC information systems using their C&A tools.

For MAR corporate support, Mr. Pham provides in-house support services including creates images of computers for future reimaging purposes, unlocks Domain accounts and password resets, encrypts computers for security following federal and agency standards. He updates web pages using XML and HTML. He modifies or creates data transformation style sheets using XSL. Mr. Pham assists with network troubleshooting for the corporate network and help set up wireless network. He creates automatic backups on each computer and performs periodic checks to make sure they are working correctly. He identifies and solves printer and copier issues for office network. He addresses all individual computer problems as needed such as difficulty printing, lost internet connection, computer errors, email setup and installation. He researches new technologies, computers and their components, and new products.

IT Support Assistant — *September 2006 – Present*

As an IT Support Assistant, Mr. Pham installs software and hardware on new desktops and laptops including Deltek, Microsoft Office Suite, CardScan, RAM, Hard Drives, and more. He conducts Network troubleshooting for the office and helps with the installation of network infrastructure devices. He has created automatic backups on each computer and conducted periodic checks to ensure they are working correctly. He identifies and solves printer and copier issues for the office network. He addresses all individual computer problems as needed such as printing difficulties, lost internet connection, computer errors, email setup, and software installation. He researches technologies such as digital signage, web conferencing, and whiteboard capture systems. He performs troubleshooting, diagnostics, and remedies computer issues.

B.F. Saul Company — **May 2006 – August 2006 (3 months)**

Administrative Assistant

As an Administrative Assistant Mr. Pham maintained a daily check log of incoming checks for record. He sent faxes, made copies, and typed/edited documents and spreadsheets as instructed by supervisors. He matched receipts with company credit card (P-Card) statements every month for various departments. He prepared P-Card documents to be scanned and archived. He prepared Senior Trust Notes to be sent and filled out deposit slips for checks. He paid invoices with P-Card for various companies and services as instructed. He searched archives to locate certain documents requested for Auditors. He made reservations and arranged web-conference meetings as needed.

Name:	**Young, Christopher M.**	**Company:**	**MAR**
Labor Category:	**Information Assurance/Security Specialist (Entry-Level)**	**Employment Status:**	**Employee**
NRC Badge:	(b)(6)	**Country of Citizenship:**	**USA**
Additional Clearance (s):			

Candidates Skills/Experience Relevant to Statement of Work

SOW #	SOW Description	Candidate Qualified
8.1	Project Management	
8.2	Special Projects	✓
8.3	System Authorization	✓
8.4	Continuous Monitoring Support	✓
8.5	Data Calls	
8.6	Cyber Situational Awareness	✓
8.7	Policy, Standards and Training	✓

Summary of Skills, Experience, and Training/Certifications Relevant to Statement of Work

Christopher Young possesses over eight years of IT related experience including hardware, network engineering and vulnerability scanning and troubleshooting. Mr. Young's technical skills include: LAN connectivity troubleshooting, NTFS Permissions, Software Deployment via Group Policy, Malware Removal, and Basic Scripting. Mr. Young has performed multiple roles including System Administrator, Cyber Security Analyst and Network Administrator. Of Mr. Young's eight years experience in the IT field, the last three years have been specifically related to the preparation of C&A artifacts according to NIST standards and performing the role of Systems Administrator/Security Analyst.

Mr. Young's technical experience exceeds the minimum qualifications of the Information Assurance/Security Specialist (Entry-Level) GSA Alliant Labor Category. As a Security Specialist working on the NRC CISSS contract Mr. Young uses scanning technologies to evaluate the security posture of client systems such as SECURITY PRIME, DISA, NESSUS. Mr. Young scans networks using the specialized tools to determine the integrity of these desktops, laptops and servers. He creates Vulnerability Tracking Sheets, Finding Tracking Sheets, Quarterly Scan Reports and other documentation as a result of scanning activities. He assists in compiling the ST&E results into a report and reviews results with customers. Mr. Young supports multiple laptops, classified and unclassified, for the Computer Security Office at the NRC. Mr. Young recommends security solutions to support NRC's requirements. Mr. Young's current experience on the CISSS qualifies him to perform duties required under SOW 8.2, 8.3, 8.4, 8.6 and 8.7 for this contract.

Education, Certifications, and Training

Education

- B.S., Information Systems, University of Maryland University College (b)(6)

Certifications and Training

- NSA Blue Team Boot Camp (NETO 3016)
- Intelligence Community Directive 503: Information Technology Systems Security Risk Management, Assessment and Authorization for the IC
- MCP, MCPS, MCNPS, MCTS
- MS Small Business Specialist (MS Exam 70-282)
- MS Forefront Client and Server, Configuring (MS Exam 70-557)
- MS Office SharePoint Server 2007, Configuring (MS Exam 70-630)
- MS Configuring Microsoft Windows Vista Client (MS Exam 70-620)
- CompTIA Security+

Name:	Young, Christopher M.	Company:	MAR
Labor Category:	Information Assurance/Security Specialist (Entry-Level)	Employment Status:	Employee

Related Experience: Professional Career Experience

MAR, Incorporated — **November 2009 – Present (2.6 years)**
System Administrator/Security Analyst

On the CISSS contract supporting NRC, Mr. Young performs the role of Security Analyst and assists in the preparation of C&A artifacts following NIST and NRC standards. He conducts security reviews using DISA, CIS, and NIST STIGs. He utilizes scanning technologies to evaluate the security posture of client systems (Secutor Prime, DISA, Nessus). Mr. Young scans networks using specialized tools such as Nessus, Hailstorm, DISA Gold Disc, and Core Impact. In support of the MAR scanning team for CISSS he creates Vulnerability Tracking Sheets, Finding Tracking Sheets, Quarterly Scan Reports and other documentation as a result of scanning activities. He prepares and reviews results with the customer for ST&E related activities. He manages multiple laptops, classified and unclassified, for the Computer Security Office at the NRC. Mr. Young was selected by the NRC to receive NSA Blue Team Boot Camp training and successfully completed the course.

In support of MAR corporate activities Mr. Young rebuilds desktops, servers, and laptops and upgrades computer hardware. Mr. Young hardens servers and computers using hardening standards provided by DISA and NIST. He creates images of computers for future reimaging purposes. He unlocks domain accounts and password resets. He performs network troubleshooting for office and helped set up corporate wireless networks. Mr. Young creates automatic backups on each computer and makes periodic checks to verify they are working correctly. He monitors, logs and proactively addresses server issues. He configures Backups via Backup Exec and remote agents. He manages spam and email attached malware via Symantec Mail Security. He installs software and hardware on new desktops, laptops, and servers.

OMNI Solutions Group — **December 2004 – October 2009 (4.8 years)**
Network Engineer

At the OMNI Solutions Group, Christopher Young preformed the role of Network Engineer and monitored, logged and proactively addressed server issues. He secured websites, file shares, and FTP sites using NTFS Permissions, Security Groups, and Active Directory. He configured Backups via Backup Exec and remote agents. He managed spam and email attached malware via Antigen/Forefront and Barracuda. He used Client Software Deployment via Group Policy. He installed and maintained MS Exchange 5.5, 2000, 2003 and 2007. He setup and utilized site-to-site and global VPN client technologies using SonicWALL firewalls.

NCR — **September 2004 – July 2005 (9 months)**
Help Desk Analyst

At NCR, Christopher Young preformed the role of Help Desk Analyst where he was the Log Technician for arrival/departure times. He troubleshot issues involving installation of cash registers and software. He worked as phone support for self checkout unit installation. Lastly, he scheduled SCSI recoveries for Post Office Network

MAY Company – GLDC — **June 2004 – August 2004 (3 months)**
Help Desk Analyst

At MAY Company - GLDC, Christopher Young preformed the role of Help Desk Analyst where he was the remote administration of multiple systems (Bridal Kiosks, PCs, and cash registers). He troubleshot terminals through TANDEM and IBM Telnet Sessions. Lastly, He created Problem Management Records (PMR) and Call Tickets to tract issues.

2.1.3.3 Computer Forensic Intrusion Specialists

Name:	**Brody, Bruce A.**	**Company:**	**CACI**
Labor Category:	**Computer Forensic and Intrusion Analyst**	**Employment Status:**	**Employee**
NRC Badge:	(b)(6)	**Country of Citizenship:**	**USA**
Additional Clearance (s):			

Candidates Skills/Experience Relevant to Statement of Work

SOW #	SOW Description	Candidate Qualified
8.1	Project Management	
8.2	Special Projects	✓
8.3	System Authorization	
8.4	Continuous Monitoring Support	
8.5	Data Calls	
8.6	Cyber Situational Awareness	✓
8.7	Policy, Standards and Training	✓

Summary of Skills, Experience, and Training/Certifications Relevant to Statement of Work

Bruce Brody possesses over 20 years of experience in Federal Information Security Leadership and Cyber Security Subject Matter Expertise. He is the Chief Cyber Security Strategist for the Paradigm Division Group of CACI, and is also performing in the role of Senior Security Architect for the NRC. Mr. Brody retired from the Federal Government after 25 years of service in January 2006. In his last Federal positions, he served as the Chief Information Security Officer (CISO) at the Department of Energy from July 2004 to January 2006, and as CISO for the Department of Veterans Affairs from March 2001 to July 2004. He holds a master's degree with an emphasis on information security and he is also a graduate of the Defense Systems Management College's Advanced Program Management Course. He is also a Certified Information Systems Security Professional (CISSP), and a Certification and Accreditation Professional (CAP), both of which are granted by the International Information Systems Security Certification Consortium $(ISC)^2$; and a Certified Information Security Manager (CISM), which is granted by the Information Systems Audit and Control Association. He is also one of the few holders of the Information System Security Professional Certification Scheme (ISSPCS), and Australian credential, as well as the newer Certified FISMA Compliance Professional (CFCP), issued by the FISMA Center.

Mr. Brody's experience and current work on the CISSS contract exceeds the requirements for the Computer Forensic and Intrusion Analyst GSA Alliant SB labor category. Mr. Brody has served as Chief Technology Officer for CACI's largest business group and corporate SME on Federal information security and related subjects. Supported Federal Chief Information Security Officers and their staff in improving the security posture of Federal enterprises, performing security architecture support, developing continuous monitoring strategies and implementations, conducting enterprise-wide risk assessments and reducing vulnerabilities across geographically diverse enterprises. Assisted one Federal enterprise in establishing its first-ever incident analysis and response center. Participated in Federal boards and committees that influenced the legislative changes that reformed FISMA.

Mr. Brody has extensive experience in IT Security Architecture and as such meets and exceeds the requirements set forth in the SOW areas 8.2, 8.6, and 8.7. Related to SOW area 8.2, Mr. Brody was responsible for leadership and direction, policy and oversight, and external reporting requirements for all of the Department's cyber and information security initiatives and programs. He. significantly improved the Department's Cyber Security posture by creating and leading enterprise-wide Cyber Security programs such as the Authentication and Authorization Infrastructure, to issue over 150,000 smart cards for logical and physical access for the Department's federal and contractor employees; Asset Management, to inventory all information systems and manage the security configurations down to the desktop; and the Cyber Security Portal, a model knowledge management tool for best practices, compliance management and governance.

Name:	Brody, Bruce A.	Company:	CACI
Labor Category:	Computer Forensic and Intrusion Analyst	Employment Status:	Employee

Mr. Brody has been approved by NRC senior CSO leadership to perform in the role of Senior Security Architect and is performing those duties in NRC today. Related to SOW area 8.6, Mr. Brody has established and operated two CIRC at two cabinet level departments, and currently supports one at Federal Communications Commission defining their policies, procedures, concept of operations and daily work breakdown. Lastly, related to SOW area 8.7, Mr. Brody has written department level policies and procedures as well as component level policies and procedures for two Government Agencies and currently for the FCC. He currently is a part of the Government Advisory Board for CISSP candidates where he implements training across many agencies in various technical and managerial levels. Mr. Brody currently holds an International Information Systems Security Certification Consortium $(ISC)^2$.

Education

- "Leadership for a Democratic Society", Federal Executive Institute, (b)(6)
- M.S., Information Security, Eastern Michigan University, (b)(6)
- B.A., History, Franklin and Marshall College, (b)(6)

Certifications and Training

- Certified FISMA Compliance Professional (CFCP) #112268, 2009
- Certified Level III Program Manager, Department of Energy (2005), Department of Veterans Affairs (2002), Department of Defense (1996)
- Certified Authorization Professional (CAP), #20474, 2007
- Information System Security Professional Certification Scheme (ISSPCS) #109, 2007
- Certified Information Security Manager (CISM), #0300286, 2003
- Certified Information Systems Security Professional (CISSP) #20474, 2000
- Defense Systems Management College, Defense Acquisition University, Level III Program Management Certification, 1995

Related Experience: Professional Career Experience

CACI, Inc. **2006 – Present (6 years)**

Vice President, Information Assurance and Chief Cyber Security Strategist

Serve as Chief Technology Officer for CACI's largest business group and corporate SME on Federal information security and related subjects. Support Federal Chief Information Security Officers and their staff in improving the security posture of Federal enterprises, performing security architecture support, developing continuous monitoring strategies and implementations, conducting enterprise-wide risk assessments and reducing vulnerabilities across geographically diverse enterprises. Assisted one Federal enterprise in establishing its first-ever incident analysis and response center. Participated in Federal boards and committees that influenced the legislative changes that reformed FISMA.

Consultant **2008 – 2011 (3 years)**

Subject Matter Expert and High-End Cyber Security Consulting

Known as the "elder statesman" of the Federal Chief Information Security Officer (CISO) community. Provided mentoring for various Federal CISOs on their duties and challenges. Performed comprehensive Federal consulting for $(ISC)^2$ and high-end consulting to the Department of Homeland Security on FISMA reform implications. In addition, played an instrumental role in the impending legislative revision of the Federal Information Security Management Act (FISMA). Provided subject matter expertise, market analysis and Federal trends and developments support for all aspects of Cyber Security for various financial management firms. Prepared business development pipelines for a number of companies focusing on the Federal Cyber Security market and arranged and facilitated meetings with key Federal officials. Selected to serve on the first Federal Advisory Board for Fortinet and Invincea. Published "thought leadership" pieces in GovInfoSecurity.com and Fierce Government IT. Selected to speak on FISMA reform for the fourth straight year at the annual RSA Security Conference 2010 in San Francisco.

Name:	Brody, Bruce A.	Company:	CACI
Labor Category:	Computer Forensic and Intrusion Analyst	Employment Status:	Employee

Department of Energy **July 2004 – January 2006 (1.5 years)**
Associate Chief Information Officer (CIO) for Cyber Security
Chief Information Security Officer (Grade: ES-2210-04)

Responsible for leadership and direction, policy and oversight, and external reporting requirements for all of the Department's cyber and information security initiatives and programs. Significantly improved the Department's Cyber Security posture by creating and leading enterprise-wide Cyber Security programs such as the Authentication and Authorization Infrastructure, to issue over 150,000 smart cards for logical and physical access for the Department's federal and contractor employees; Asset Management, to inventory all information systems and manage the security configurations down to the desktop; and the Cyber Security Portal, a model knowledge management tool for best practices, compliance management and governance.

Department of Veterans Affairs, **March 2001 - July 2004 (3.3 years)**
Associate Deputy Assistant Secretary for Cyber and Information Security
Chief Information Security Officer (Grade: ES-0301-03)

Personally responsible for developing and managing large-scale, nationwide programs, such as (1) reducing the number of Internet gateways from over 200 to 4, centrally managed and monitored 24x7, resulting in a significant hardening of network boundaries; (2) establishing the largest integrated anti-virus regime in the government; (3) training, qualifying, testing, certifying and credentialing 600 information security practitioners; (4) initiating a comprehensive security configuration management program to centrally manage vulnerabilities; and (5) assuring the business lines of the largest integrated hospital system in the world and the 5th largest financial/insurance system in the United States. Took the Department from an "F" to a "C" on its annual Congressional Report Card and recognized as a "Federal 100" recipient in 2004.

Office of the Assistant Secretary of Defense for C3I, The Pentagon **1996 – 2001 (5 years)**
Director, Information Superiority Investment Strategy (ISIS) 1998 - 2001
Acting Director, Technical Integration 1997 - 1998

Conducted comprehensive, performance-based, modeling and simulation and technical evaluation of the DoD's over $50 billion annual budget in command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) programs, resulting in $1.5 billion of redirected funding to optimize portfolio investment. Findings resulted in increases for national security systems funding to support operational combat outcomes.

Defense Information Systems Agency (DISA), Arlington, VA **1993 – 1996 (3 years)**
Chief, Joint C4I Decision Support Center 1996
Chief, Joint Information Management Center (JIMC) 1996
Chief, Multilevel Security Division 1993 - 1995

Created first-ever Joint Information Management Center (JIMC) in support of Bosnia peacekeeping operations, enabling the "push" and "pull" of multiple classification levels of information to and from Bosnia to improve information management and knowledge management capabilities. Directed the DISA Multilevel Security (MLS) Division and the DoD MLS Program. Delivered successful MLS implementations at military commands, enabling secure connectivity between TS/SCI-level intelligence environments and Secret-level command and control environments. This pioneering effort resulted in the creation of the Cross Domain Program Management Office (CDPMO) in existence today.

Name:	**Ruf, Brian J.**	**Company:**	**CACI**
Labor Category:	**Computer Forensic and Intrusion Analyst**	**Employment Status:**	**Employee**
NRC Badge:	(b)(6)	**Country of Citizenship:**	**USA**
Additional Clearance (s):			

Candidates Skills/Experience Relevant to Statement of Work

SOW #	SOW Description	Candidate Qualified
8.1	Project Management	
8.2	Special Projects	✓
8.3	System Authorization	
8.4	Continuous Monitoring Support	
8.5	Data Calls	
8.6	Cyber Situational Awareness	✓
8.7	Policy, Standards and Training	

Summary of Skills, Experience, and Training/Certifications Relevant to Statement of Work

Brian Ruf has over 21 years of professional experience in Cyber Security, Architecture and Information Assurance management. In addition, Mr. Ruf holds a PMP certification and is a Certified Information System Security Professional (CISSP). Mr. Ruf successfully bridges business acumen with a solid understanding of technology implementation and operations to architect, consult, and lead efforts related to Cyber Security, information assurance, and regulatory compliance. He applies experience and expertise with methodologies such as ISO-9001, SE-CMM/CMMi, System Development Life Cycle (SDLC), and Enterprise Architecture to achieve realistic and sustainable structures which ensure the long-term success. Mr. Ruf's professional experience is enhanced by his excellent communication, presentation and leadership skills.

Mr. Ruf's over 21 years in the Cyber Security field, as both an IT Security Architect and Manager exceeds the minimum qualifications for the Computer Forensic and Intrusion Analyst GSA Alliant SB Labor Category. In his role as Cyber Security Architect, Mr. Ruf conducts Vulnerability Assessments, along with penetration testing with systems. Mr. Ruf has also led Regulatory Compliance efforts to establish and evolve consistent records handling practices.

Mr. Ruf has extensive experience in IT Security Architecture and as such meets and exceeds the requirements set forth in the SOW areas 8.2, 8.6 and 8.7. Related to SOW 8.2, Mr. Ruf has defined and coordinated implementation of security strategies based on the firm's strategic business plan, industry practices and risk-assessment-based decision making. Mr. Ruf developed an internal whitepaper that assessed and documented firm-wide information handling from a systemic and evolutionary perspective. This paper kicked off a multi-million dollar, multi-year initiative within the firm. He has knowledge in best practice evaluation in regards to new technology. Mr. Ruf's strength in SOW 8.6 and 8.7 is related to his experience of defining and implementing enterprise security architecture (ESA) programs for Federal civilian agencies, such as Customs and Border Protection, and Fortune 500 companies. Early in his career, Mr. Ruf was an IT practitioner in the fields of software development, network engineering and end-user support. This background provides real-world context to his application of more conceptual practices. Mr. Ruf's experience, combined with his program and project management success, and seasoned consulting skills make him an excellent candidate to produce Enterprise Architecture deliverables.

Education, Certifications, and Training

Education

- B.S., Information Science, The Richard Stockton College of New Jersey (b)(6)

Certifications and Training

- Project Management Professional, PMI, 2008
- Certified Information System Security Professional (CISSP), 2000

Name:	Ruf, Brian J.	Company:	CACI
Labor Category:	Computer Forensic and Intrusion Analyst	Employment Status:	Employee

Related Experience: Professional Career Experience

CACI, INC. – FEDERAL **August 2010 – Present (1.8 years)**
Cyber Security Architect
As a Cyber Security Architect, Mr. Ruf is responsible for designing and managing the development of pre-packaged information assurance solutions that facilitate effective deployment for our customers at a fraction of the time and cost normally required.

Booz Allen Hamilton **September 2008 – July 2010 (1.8 years)**
Records & Information Management (RIM) Program Manager (Internal Operations)
Mr. Ruf led regulatory compliance efforts to establish and evolve consistent records handling practices throughout the firm that were efficient, effective and compliant. He reduced record footprint dramatically throughout the firm through a combined approach of strategic planning, opportunity tracking, policy development/implementation, process integration, targeted training and awareness efforts, and ongoing guidance activities. Mr. Ruf turned the program around from one with which no organization wanted to interact, to one which most organizations actively pursued for guidance and support.

Booz Allen Hamilton **March 2007 – August 2008 (1.5 years)**
Records & Information Management (RIM) Architect (Internal Operations)
As a Records and Information Management (RIM) Architect, Mr. Ruf developed strategy and solutions in support of a previous manager.

Booz Allen Hamilton **January 2005 – February 2007 (2.1 years)**
IT Security Architect (Internal Operations)
As an IT Security Architect, Mr. Ruf defined and coordinated implementation of security strategies based on the firm's strategic business plan, industry practices and risk-assessment-based decision making. Mr. Ruf developed an internal whitepaper that assessed and documented firm-wide information handling from a systemic and evolutionary perspective. This paper kicked off a multi-million dollar, multi-year initiative within the firm.

CACI Technologies, Inc. **August 2003–January 2005 (1.4 years)**
Program Manager - Information Assurance - Commercial
Mr. Ruf managed all matrixed IA resources and all commercial IA clients including a Fortune 50 customer. He defined and implemented the security program and System Development Lifecycle Methodology (SDLC) for a global telecommunications provider, and led an internal effort to institute ISO-9001 compliant IA processes such as risk assessment and patch management as offerings to clients.

CACI Technologies, Inc. **August 2001–August 2003 (2 years)**
IT Security Architect (Customs and Border Protection)
Mr. Ruf developed the security aspects of the enterprise architecture capability, defining and integrating processes that ensured secure and compliant execution of their System Development Lifecycle (SDLC) and Project Management Methodology (PMM), including integration with the existing Technical Reference Model, emerging SE-CMM processes, and the creation of their IT Security Solutions Catalog.

SRA International **July 2000 – July 2001 (1 year)**
Sr. Information Security Engineer
Mr. Ruf served as the security lead and deputy technical lead for the US Exports Interagency Program Management Office, a Congressionally funded effort to modernize the US Export Licensing Process. He designed and managed initial deployment of SRA's first Information Assurance Lab. Mr. Ruf designed a complete and fully compliant security program plan for the Pension and Welfare Benefits Administration (PWBA), which the Department of Labor's (DOL) CIO, adopted as the standard for every DOL agency.

Department of Transportation/Federal Aviation Administration
Computer Specialist **January 1990 – June 2000 (10.5 years)**
Mr. Ruf represented the support organization on all security development, implementation and operations of the (then) new air traffic control (ATC) system, STARS, performing risk assessment, technical & procedural mitigation, and training & awareness activities. Mr. Ruf also developed and implemented cross-system communication capabilities, and support efforts to extend the life of the aging ARTS-IIIA air traffic control system.

2.2 Staffing, Recruiting, and Retention

2.2.1 Staffing

Through our past experience as a contractor for the NRC, and our thorough understanding of the required support services requested in the CSPSS RFQ, we will continue to be very deliberate in selecting and retaining personnel who have the proven ability to successfully perform their tasks on schedule and in accordance with strict performance requirements. In this regard, we employ the use of a our internally developed **Staff Management Process** which entails weekly meetings between our CISSS Project and Financial Managers and our Human Resources and Recruiting staff to assess staffing levels and requirements. We keep track of all MAR and subcontractor personnel in an organizational chart according to task order assignment. This chart is reviewed and updated on a weekly basis with a view toward making sure that task orders are adequately staffed and that individuals are not over or under utilized. This analysis is compared to existing and anticipated **Project Plans,** as discussed in Section 1.A.2.1, to add the dimensions of time and funds remaining in order to complete assignments on schedule and within budget. Personnel resources can then be adjusted as deemed appropriate. Our TaskTracker System serves as the financial backbone of this process by keeping track of time, dollars expended, and progress toward task order completion. Using this process supported by data from TaskTracker, our Project and Financial Managers will be able to consistently communicate with our NRC customers to give them a comfort level about resources available and task order status as well as our ability to meet future requirements.

Through lessons learned, we have worked with the Program Offices to locate qualified and technical staff to perform specific program activities in support of their needs. We have also removed personnel from the contract in instances where their skill sets do not match upcoming requirements.

Our current Team, along with newly added team members, will be ready to immediately transition to the CSPSS project, without any disruption to the ongoing NRC Cyber Security Program. We are constantly recruiting for emergent staffing requirements, and our Team has an established network of technical resources that will be used to meet core, special, and surge type of requirements.

2.2.2 Retention of Employees

Our Team has a strong commitment from the top management at each member company to create a challenging and enjoyable workplace for our employees. At MAR, we take pride in being an "employee associate oriented" company, respecting each employee and their rights as a worker while furnishing a working environment conducive to career progression and advancement. MAR's ability to retain quality technical personnel is the result of our management philosophy and environment. Successful employee retention begins with careful recruiting. Only individuals who can potentially grow within the company and are a good fit for task order requirements are considered for employment. Individuals must possess the education, technical skills, experience, and personality traits required to do the job.

By paying attention to the needs of our employees we have been able to develop an outstanding record of retaining quality personnel. MAR offers attractive compensation and benefits. Our wage and salary structures are very competitive and our benefit plans are reviewed and updated regularly. We host "brown bag" lessons learned luncheons which focus on a variety of technical topics such as specialized NRC centric training for the use of Nessus ProFeed, POA&M scorecard process overviews, and template change overviews, where past work is evaluated and process improvements are discussed. Time spent together this way leads to high morale, excellent employer-employee relations, and a motivated team that provides outstanding performance. Salary levels and bonuses are reviewed and adjusted periodically as a means of monitoring labor market conditions and economic factors to ensure MAR's maintains its competitive marketplace position.

We are committed to rewarding employee excellence and dedication, and are proud of the fact that over 50% of job vacancies are filled through internal promotions or employee referrals.

2.2.3 Training

We have found that a genuine effort to improve employee skills and technical education helps in maintaining high morale, promotes career advancement, and directly benefits our customers. Recently, we determined that employees working in the Cyber Security related field should become ITIL certified. MAR hired an instructor for 20 of our employees in order for them to complete the basic ITIL training program. The training was held at MAR over a long weekend and all employees who participated successfully passed the exam at the end of the training program. We have decided to continue to expand the levels of ITIL training that our employees can obtain and will be holding future training classes. We have also provided employees with PMP, SANS GSEC, and other related training.

We often send our personnel to local conferences, seminars, and training classes to promote awareness of current or new developments in the specialized technical areas they support. Employees are also encouraged to join local and national user and professional groups relevant to their career path.

During the on-boarding process, emphasis is given to the importance of upward mobility, internal promotions, and mentoring. Employees receive an overview of the types of training programs we have in place to advance their education. To share experience among staff and to foster cross training for key work areas, MAR coordinates employee events and luncheons where employees share this new technology and day-to-day work experiences.

We also support technical training of employees by offering tuition reimbursement for college-level courses. We assist in paying for approved work related courses. MAR also pays the full cost of any technical and management development seminars and workshops that employees are approved to attend. On-line training is also provided to minimize time away from the workplace.

3.0 CORPORATE EXPERIENCE

RFP Section E, pages 5-6

MAR, together with our team members, have over 150 years of experience supporting the Federal Government along with an established foundation in Cyber Security, Information Technology, and Program Management. MAR provides Cyber Security services to the NRC, the Intelligence Community, Naval Facilities Engineering Service Center East Coast Detachment, and the Office of Personnel Management. MAR's team members provide Cyber Security services to Federal agencies that include the Department of Commerce, Office of the Secretary of Defense, US Army, Transportation Security Administration, DHS, Department of Education, Defense Intelligence Agency, Health and Human Services, USDA, Department of Transportation, Housing and Urban Development, and others. Through a partnership with our team member, the University of Maryland's Maryland Cybersecurity Center (MC2), we will have access to an interdisciplinary research center with expertise in wireless security, cryptography, software assurance, supply chain security, multimedia forensics, and other innovations to address the cyber security threat. Our combined Team is positioned to support the day-to-day NRC cyber security activities, as well as provide a strong diverse set of capabilities to undertake special projects, new business solutions, and innovative approaches to cyber security training and communications.

The MAR CSPSS Team will be located in Rockville, Maryland at MAR's current NRC CISSS project facility (1803 Research Blvd) which is roughly 5.5 miles from the NRC's Headquarters. This project office facility is dedicated to housing MAR's NRC Team and is on the same floor as

MAR's Headquarters. The facility is physically separated from MAR Headquarters with access only granted to individuals that have an NRC badge. The network within the MAR NRC facility is also separated from the MAR corporate network. All laptops, network devices, and media are configured to comply with the requirements outlined in SOW Section 9 - IT Cyber Security Requirements. MAR maintains an inventory of laptops computers solely for use on the NRC project. Each laptop is encrypted using an NRC approved, FIPS 140-2 validated product. We require each subcontractor to also follow the same guidelines for laptops provided to their staff.

MAR Team members on the contract have dedicated desks and hotel cubes to accommodate surge staff. The facility has a conference room set up with a large white board and a projector to accommodate meetings, collaboration sessions, training dry runs, lessons learned sessions, and other activities to enhance project execution and communication. Being located down the hall from MAR HQ, MAR's Project Management Team has direct and immediate access to corporate resources including the CEO, Human Resources, Contracts, and Accounting to quickly address any issues or surge needs for the project. To further support the project all key MAR executives are NRC cleared with badges. This includes, the MAR CEO - Michael Norcio, VP of Cyber Security and IT Services - Samuel Sunukjian, VP of HR and Administration and ISO Quality Manager - Laura Evans, VP of Contracts - Linda Klages, Senior VP of Systems Engineering and Integration and Chief Technology Officer - Daniel Hackenberg, and MAR's Facility Security Officer (FSO) - Gayle Enfinger. To ensure our ability to respond to the NRC, MAR currently provides monthly parking passes to the Team at a parking facility located near the NRC HQ campus.

3.1 Project Management (SOW Task 8.1)

MAR has an established NRC experienced and certified Project Management Team. They are currently managing a diverse team ranging in size from 25-40 individuals across 78 task orders covering 26 functional task areas. MAR's commitment to supporting our customers responsibly and ethically has resulted in a solid history of efficient time, budget, resource management, and a team dedicated to seeking additional efficiencies each time they take on new tasks. For CSPSS we will augment the management team with a Technical Quality Assurance Lead and a second Project Manager. This Management Team along with our existing analysts and SMEs are available to immediately transition to the CSPSS project.

Quality Assurance Plan: For QA we have developed a QA Handbook, providing step-by-step instructions for verifying the accuracy of each type of deliverable, formatting and editing checklists used to ensure that deliverables comply with NRC required formats and templates, and process monitoring checklists used to make certain that staff follow MAR established processes throughout the duration of each project. Corrective and preventive actions are documented during lessons learned meetings. Both MAR and CACI have ISO 9001:2008 certification, and team members such as CACI and DCCA are Capability Maturity Model Integration (CMMI) appraised and use these methodologies to build quality into service delivery.

Project Plan: As outlined in Section 1.A.1 we will continue our use of TaskTracker to support the daily technical and financial management aligned with the work breakdown structure in the project plans. TaskTracker was developed to support the NRC CISSS contract and has been successfully deployed to support other MAR contracts. MAR's Project Management Team also uses internal SharePoint portals to track and disseminate project schedule and related information to the team. For example, under the CISSS contract MAR tracks initial ATOs and key FISMA compliance milestones using the FISMA Tracker Dashboard. Scanning schedules, tools, and guidance are provided on the Scanning Dashboard. Contract guidance per the SOW, Project Officer Direction, and internal policy and procedures are also disseminated via the SharePoint portal.

3.2 Special Projects (SOW Task 8.2)

Residual Risk Assessment: MAR Team member KCG has demonstrated experience developing residual risk assessments including the preparation of Designated Approving Authority (DAA) briefing packages that outline the current risk level of the information systems. The result is a risk-based recommendation for the system's authority to operate. KCG has provided this service to numerous agencies including over two years of experience supporting the NRC.

Classified Processing Support: MAR along with team members CACI, DCCA, Prometheus and Securicon have experience in supporting classified systems. As outlined in MAR's past performance reference for the Intelligence Community, we are responsible for the oversight of C&A, Continuous Monitoring, and reaccreditation for 120 systems. MAR's technical staff is familiar with the Committee on National Security Systems (CNSS) and Director of National Intelligence issuances, and has access to technical expertise of the senior security analysts supplied by our teaming partners. CACI, a longstanding security service provider, brings a team of qualified, certified cyber security professionals – 35% holding DoD Top Secret (TS) clearances, and over 20% hold TS/SCI clearances, many with CI and Full Scope polygraphs.

Evaluation of New Technologies: MAR has assisted the NRC with the evaluation of new technologies, including the use of a cloud-based, automated application security testing software service. This service assesses static binary code and dynamic applications for security vulnerabilities. The associated security devices were used to assess the risk posed to the agency by Advanced Persistent Threat (APT) attacks, and tools used to assess web applications. CACI's Cyber Solutions Lab has been used by numerous Federal agencies as a platform to evaluate new technologies and to perform comparative analysis on cyber security tools. This lab will be available to the NRC under CSPSS. Through KCG's FedRamp 3PAO accreditation our team offers a cloud computing assessment capability for the NRC.

Analysis of Best Practices: MAR has analyzed security best practices and developed white papers with recommendations concerning application of the practices to the NRC Cyber Security Program. For example, MAR researched best practices in meeting E-authentication assurance requirements (including the five step process outlined in OMB 04-04), and analyzed them in the context of NRC system security categorizations. NRC stakeholders considered these recommendations during subsequent security categorizations. MAR's team member, KCG is also responsible for recommending industry best practices for NRC security processes.

3.3 FISMA Compliance and Oversight (SOW Tasks 8.3, 8.4, 8.5)

Obtaining Authorization to Operate: MAR has worked closely with the NRC to consistently achieve ATOs for their operational systems. The support included developing the full authorization lifecycle of security artifacts. We have worked with the NRC in moving toward alignment with the NIST Risk Management Framework model. MAR Team members KCG, Securicon, Mainstay, and Prometheus have provided comparable services to a wide range of Federal Civilian, DoD, and Intelligence Community organizations.

Laptop Authorization to Operate: In addition to application system ATO support, MAR has assessed NRC laptops for the purpose of supplying system owner's with the documentation required to obtain laptop ATOs from the NRC DAA.

Continuous Monitoring Support: In support of the current NRC continuous monitoring process, MAR has maintained a FISMA Tracker portal to simplify scheduling of continuous monitoring activities, and an EVM system providing the daily metrics required to efficiently meet deadlines while staying within project budgets. MAR has also conducted ASCTs per NIST 800-53 and NRC-defined

Cyber Security requirements. At the enterprise level, MAR has assessed the agency's common and hybrid controls annually. On a quarterly basis, MAR has conducted vulnerability scans of the systems MAR supports under the CISSS contract using CSO-approved tools and explicit or implicit NRC Cyber Security Configuration standards. MAR has worked closely with System Owners to identify mitigation strategies for those vulnerabilities that cannot be completely remediated. Using the Quarterly Scan Report we work with the System Owners to identify the open vulnerabilities that must be added to the system's POA&M report.

Data Calls. MAR has always been available on short notice to assist NRC when responding to Cyber Security-related data calls from the NRC OIG, DAA, or System Owners. Our onsite embedded resources and close proximity to the NRC campus ensure a prompt response to urgent requests.

3.4 Cyber Situational Awareness (SOW Task 8.6)

Incident Response: MAR has supported the NRC CSA Team in tracking and reporting of Incident Responses. We have developed an insight on the trends of incidents that occur at the NRC. MAR Team members CACI, Prometheus, and Securicon have developed and supported IR programs at other government agencies and will bring these best practices to the CSPSS Team.

NRC Enterprise Security Architecture: In support of the NRC CISSS contract MAR prepared an Enterprise Risk Assessment (ERA) which identified areas in the infrastructure that are particularly vulnerable to security incidents. From the ERA and other data points MAR is assisting the NRC in building an ESA with the objective of facilitating an appropriate risk based strategy for protecting NRC data and information systems. MAR's team member, Prometheus, also brings years of innovative experience in network security at the enterprise level. Over the past decade CACI's senior architect Brian Ruf has been supporting agencies such as the Department of Commerce in developing and refining their ESA.

Source Code Reviews: MAR is working with the NRC in identifying, assessing, and obtaining authorization to use a variety of security solutions. MAR is supporting the NRC in the evaluation of offsite SAAS used to analyze and assess static binary code and dynamic applications for security vulnerabilities. We have a number of experienced, NRC cleared, software developers that can be called upon to verify the capabilities of system development auditing tools used throughout the agency. CACI's Cyber Solutions Lab provides a collaborative environment with interactive tools that allow clients to visualize and test proposed information assurance and security solutions before implementing them. The lab hosts a significant inventory of network devices and monitoring applications. As a technology agnostic company, CACI can identify the best candidate among vendors that meet NRC's needs. The lab is used to test potential vendor solutions, which are then tailored and demonstrated to their customers.

Penetration Testing: MAR has assisted the NRC with external "red team" and internal "blue team" penetration testing and social engineering tests targeted at the NRC IT infrastructure and users. Tests were planned in detail, approved by the NRC, and conducted in the presence of an NRC representative. In addition to MAR's experience at the NRC, Michael and Scott Shinn of Prometheus were members of the first commercial penetration testing team during their tenure at Cisco. MAR's team member, CACI, has developed an integrated Insider Threat Detection Programs that can assist in the planning, establishment, and sustainment of an Insider Threat Detection Program for other federal agencies. The program offers insider threat assessments, policy development, and sustainable Insider Threat Detection Program operational support. KCG has established penetration testing "fly-away" teams that are focused on rapidly developing and executing penetration testing geared toward specific customer requirements.

Security Impact Assessments: MAR has assisted NRC System Owners with incorporating changes to their authorized systems via the NRC SIA process. MAR assists System Owners by interpreting guidance from the NRC by informing them of required system documentation updates. MAR has also conducted the vulnerability assessments required to ensure that the change does not adversely impact the system or NRC infrastructure security posture. MAR's team member KCG has recommended comparable SIA solutions to many of their customers.

3.5 Policy, Standards, and Training (SOW Task 8.7)

Cyber Security Policy: MAR has supported key CSO stakeholders with updating the recent revision to Management Directive and Handbook (MD) 12.5 to ensure that the directive addresses all federally mandated requirements. The directive uses the framework developed by the ISO/IEC Standard 27002:2005(E), and addresses each of the main security categories within the standard. MAR provided a number of staff resources each with specific knowledge and skills needed to research and address sections of MD 12.5.

Processes, Procedures, Templates, Checklists, Standards, and Guidance: MAR supported the NRC CSO when it established a SWG, a forum for stakeholders to provide input into the standards development process and standards road map, and discuss operational or technical concerns before standards became effective. With input from the SWG and direction from CSO, MAR developed CSO-STD-0020, "Organization Defined Values for System Security Controls" which provides the NRC-required values for specific security controls identified in federal computer security control standards and guidance.

Security Relevant Business Solutions: CACI's expertise in developing Information Technology and Information Assurance solutions provides our team skills in evaluating secure business processes. MAR's security analysts have also evaluated and briefed the NRC on the capabilities and benefits of a variety of assessment and vulnerability scanning tools. This combined experience equips our Team to better identify and document solutions that enable secure NRC business processes.

Cyber Security Awareness Programs: MAR Team member Mainstay has over 15 years of experience providing Training and Cyber Security awareness services on Army contracts. Results from MAR's work on the NRC PhishMe task provided information that has been incorporated into NRC security training and awareness programs.

Cyber Security Role-based Training Program: MAR has developed and delivered role-based training for NRC System Administrators, Information System Security IT Managers, Executives and System Owners, and ISSOs. We have performed this service at the NRC for a number of years both as a subcontractor and prime contractor. Participant Manuals and Lab Workbooks were developed by MAR and provided to each class. The hands-on approach was used to familiarize the class with key Cyber Security topics and resources applicable to their specific roles at the agency.

Cyber Security Conference: MAR was a key organizer and participant in the University of Maryland's Commercial Nuclear Power Cyber Security Conference held on May 4 and 5, 2011 in College Park, Maryland. Academic leaders at the university together with individuals from the NRC, commercial nuclear power industry, and private sector met to explore new regulatory and industry-led initiatives to protect nuclear power plants from cyber-based threats. MAR's proposed Program Manager, George Simonds, was a co-chair of the organizing committee.

Electronically Communicating Cyber Security Information: KCG's work at the TSA included the development and ongoing support of a cyber security newsletter to communicate new cyber threats and changes to the Cyber Security Program at the administration. MAR has supported newsletter development and web site content maintenance for its DOI customer.

4.0 PAST PERFORMANCE

RFP Section E, pages E-6 and E-7

4.1 List of Contracts (RFQ Attachment E)

1. Firm Name & Address: **MAR, Incorporated**, 1803 Research Boulevard, Suite 204, Rockville, MD 20850	2. Year Firm Established: 1971	3. Date Prepared: June 27, 2012
4. Type of Firm: X A. Small Business __B. Small Disadvantaged __C. Woman-Owned __D. Hubzone __E. Service-Disabled Veteran-Owned __F. Other (Specify)_____		
5. Principal Points of Contact: (List two by Name/Title/Current Telephone Number) Sam Sunukjian, MAR NRC Program Manager: 301-230-4567, ssunukjian@marinc.com Linda Klages, Vice President, Contracts: 301-230-4576. lklages@marinc.com		
6. Present Offices: (Address/Telephone): 1803 Research Boulevard, Suite 204, Rockville, MD 20850 I 301-231-0100		
7. Past Performance Last 3 Years: (1) List Contracts Similar in Size (Dollars) and Scope; (2) List Contracts Similar in Scope Only		
Contract No: GS-35F-0229K, Delivery Order: DR-33-06-317/IDIQ Period of Performance: 07/06 – 10/2012 Dollar Value: $41M (original value)/$49.5M (with extensions) Name of Gov./Commercial Entity: Nuclear Regulatory Commission (NRC)	Contracting Contact Name & Phone: Jordan Pulaski, Senior Contract Specialist (301) 492-3647 Technical Rep. Name & Phone: Bill Dabbs, Project Officer, (301) 415-0524	Brief Description and How it is Similar to NRC's Requirement: Please see below.

Description: MAR was awarded a $41M, five year Information Security and Cyber Security support contract by the NRC. MAR supports the NRC's Computer Security Office (CSO) to grow and strengthen its IT security capabilities for FISMA compliance. MAR performs all project management duties, including the QA of deliverables and development/management of project plans. We assembled and **manage a team of 25-40** security analysts, security engineers, network engineers, senior cyber security consultants, technical writers and support personnel. We have partnered with **11 subcontractors** to provide the depth and expertise required to support this major security engineering contract for the NRC. To date there have been **78 funded TOs**, with 31 of the TOs active and running concurrently.

Directly relevant to the CSPSS SOW are the **26 Functional Task Areas** that MAR supports for the CISSS contract which includes the following categories:

- Special Project(s) Support: MAR provides reports as requested on cyber security risks across the NRC infrastructure. We evaluate new technologies to understand their security impact and how they could be used to enhance the NRC's security program. We also analyze cyber security best practices and recommend how these practices can be used at the NRC. MAR also completed an Enterprise Risk Assessment as a Special project for the NRC.
- FISMA Compliance and Oversight: MAR assists the NRC in authorizing each of its systems to operate. We supported the establishment and assist with the maintenance of the continuous monitoring program. We support the NRC to respond to data calls from other government agencies and the NRC OIG when needed. MAR also provides assessment activities to ensure compliance with federally mandated and NRC defined cyber security requirements.
- Cyber Situational Awareness Support: MAR supports incident response efforts; performs vulnerability assessments; verifies and validates the NRC's use of SCAP; assists the NRC in evaluating tools to support the software quality program initiative; performs security penetration testing; evaluates system security designs and configurations; and we are currently supporting the development of an enterprise security architecture.
- Security Policy, Standards, and Training Support: MAR assists the NRC in developing, establishing, and maintaining Cyber Security Policies in accordance with Federal and industry best practices; assists the NRC in developing processes, procedures, templates, checklists, standards, and guidance, analyzes business solutions; establishes, conducts, and maintains Security Awareness training, role-based training, and other specialized Cyber Security training; and assists the NRC to communicate Cyber Security information to the NRC user community.

Problems/Resolutions: Difficulties were encountered in staying within the Unit-based pricing during the early phase of the CISSS contract. MAR worked with NRC to establish standardized C&A templates and we developed checklists to support the templates. In addition, MAR developed and implemented TaskTracker and TimeTracker to electronically capture and monitor daily technical and financial status. As a result of these corrective actions, unit-based work is now completed significantly below the scheduled costs.

Contract No: Task Order 004 Period of Performance: October 2008 – Present Dollar Value: This information cannot be provided due to security reasons. Please request dollar value from POC. Name of Gov./Commercial Entity: Computer Sciences Corporation (Prime) in support of the Intelligence Community at Ft. Meade.	Contracting Contact Name & Phone: Raelyn Herbert, Contracting Officer's Representative 410 654-8643 Technical Rep. Name & Phone: Kim Prentice, Applications Hosting PM 443-445-7153	Brief Description and How it is Similar to NRC's Requirement: Please see below.

Description: MAR provides the Technical Task Order (TTO) Lead Personnel for the Mission Server Support Technical Task Order. Due to the expertise and knowledge of our key personnel, MAR was selected by the prime contractor, Computer Sciences Corporation (CSC), to lead the technical effort in this area. MAR's TTO Leader oversees a 54 person System Administration/System Engineer Sustainment and Maintenance team. We are responsible for the C&A, Continuous Monitoring, and Reaccreditation activities for **120 systems** to include site visits, vulnerability assessments, mitigation actions, update of System Security Plans (SSPs) and support documentation. In addition, we manage the Incident Management Team by overseeing the cleanup of data spills, and coordinating the investigation of computer system and network security incidents with internal staff and other US Government investigators. MAR supports over 1000 pieces of mission critical hardware. These are predominantly legacy servers that are working toward being virtualized. They are currently running everything from Windows XP through Solaris 10 and Linux Redhat 5. MAR also assists with staffing the TTO and providing 24/7 call-in support to all Mission Servers. This task also provides support for current critical mission support programs.

Directly relevant to the CSPSS SOW are the Functional Task Areas that MAR supports for this task order which includes the following categories:

- Security Engineering and Certification and Accreditation (C&A): MAR provides senior level security management engineering support for our prime in support of this contract. MAR's responsibilities include implementing, providing and enforcing information security policy and guidance, and directing the development of security standard operating procedures and standard C&A body of evidence documentation. We are responsible for the C&A, Continuous Monitoring, and Reaccreditation activities for 120 systems to include site visits, vulnerability assessments, mitigation actions, update of System Security Plans (SSPs) and support documentation. In addition, we manage the Incident Management Team by overseeing the cleanup of data spills, and coordinating the investigation of computer system and network security incidents with internal staff and other US Government investigators. Our Team also ensures that server configuration compliance and security controls are in place using Opsware and other asset management tools. MAR provides direct technical security support to the customer, advising on a broad range of security topics and policies.

Other areas of support include:

- Data Center Support: MAR provides design, development, and sustainment support to the Agency's new Enterprise Data Center. This includes developing contingency plans for alternate sites so as to resume monitoring when primary site monitoring capabilities are impaired; integrating with the data center Engineering Team to design and document policies and procedures for implementation and management of both physical and virtual server platforms.
- Systems Operations, Administration, and Maintenance:
- Tier I & II Service Desk Support and 24/7/365 Operations: MAR also supplies high level Enterprise Managerial services to support real-time monitoring of critical systems.

Contract No: N00178-04-D-4081 EJP1 (Seaport-e) Period of Performance: September 2007 – September 2012 Dollar Value:$31,636,513 (ceiling) / $13,310,163 (currently funded) Name of Gov./Commercial Entity: Naval Facilities Engineering Service Center, East Coast Detachment (NAVFAC ESC ECDet)	Contracting Contact Name & Phone: Elson G. Muzada (Contract Specialist) (805) 982-2551 Technical Rep. Name & Phone: Michael (Terry) Clarke (COR) 202-433-5517	Brief Description and How it is Similar to NRC's Requirement: Please see below.

Description: This Seaport-e contract delivery order provides comprehensive technical assistance including software engineering, information assurance, system administration and security, program management, and customer service support to the Naval Facilities Engineering Service Center East Coast Detachment (NAVFAC ESC ECDet) across all product lines associated with the Ocean Construction Division. These efforts include project management services for inspections and studies conducted across the ECDet product lines, including the Waterfront Facilities product line; development and fielding of enterprise-level management and inspection reporting tools; classified system/network administration, asset configuration and system security management; development support for new data collection standards, including generation of the UNIFORMAT II standard for Naval Waterfront Facilities and Navy Dry Docks; logistical and onsite support for the Petroleum, Oil and Pipelines program; and technical and program management support for various aspects of the Fleet Moorings, Cables, Pipelines, Hyperbarics, Magnetic Silencing Facilities, Water Tanks, Bridges, and Waterfront Facilities product lines. Under this contract delivery order, MAR and our subcontractor team are developing and deploying engineering and program support tools, including Asset Management tools with GIS data and reporting capabilities, and processes to spatially index and relate facilities held in the Internet Naval Facilities Asset Data Store. A multiple toolbar with command button plug-ins that run within ESRI ArcView products has been developed and implemented and two of these extensions have evolved into comprehensive spatial database systems which continue to undergo spiral development and deployment. Efforts include system support and enhancements for application-specific geo-databases with an ArcMap custom interface for managing survey data and analysis. MAR is responsible for the full compliance to DOD/Navy accreditation and certification under DITSCAP/DIACAP requirements for the enterprise roll-out, leading to full ATO in FY 2012. Current efforts also include the development of a 3D mass model of the existing and proposed Okinawa (Marine Corps) Futenma Replacement Facility (FRF) using AutoCAD Civil 3D. This work provides direct support to the Ocean Facilities Department / Ocean Construction Division of NAVFAC ESC and demonstrates comprehensive knowledge of the inspection programs at every level from top-end program management down to the trench-level data collection and assessment. The ECDet work efforts are primarily associated with the inspection, repair and maintenance of in-water and waterfront assets for which NAVFAC ESC is directly responsible. Skill areas and personnel expertise for the NAVFAC ESC ECDet support requirements include: systems engineering/integrated logistics, database development and design, ocean engineering, waterfront facilities survey and inspection, environmental permitting, two and three-dimensional structure modeling and rendering, generation of drawings using computer-aided design and drafting, and marine technical and logistics support.

Directly relevant to the CSPSS SOW are the system security and related technical areas that MAR supports for this task order including the following:

- The development, integration, and application support of NAVFAC ieFACMAN and e-Projects applications, web-based software suites providing task project and financial management tools for tracking work efforts at the individual and program levels. Developmental support for the Ocean Facilities Information Management System (OFIMS), a facilities asset management tool with integrated GIS, engineering, inspection, media, and other data types.
- DITSCAP/DIACAP certification/accreditation coordination support with NAVFAC Information Technology Center (NITC) for the production version deployment of the OFIMS tool.
- Classified system security including the monitoring of Application, Security, and System logs; configuration and deployment of network assets, desktops and servers ; installation of system/asset updates and validation of consistent security configurations; audit and remediate systems and create automated remediation scripts based on DISA and WASSP requirements; DIACAP C&A package development support and coordination; maintain a managed antivirus environment, including updating virus definitions from the management server; create tape backup schedule and verify backups; troubleshoot issues related to MS IIS (web server) and related applications and end user technical issues.

The foregoing is a statement of facts

Signature: _____ Title: Chairman and CEO Date: June 27, 2012

1. Firm Name & Address: **CACI Federal, Inc.**, 1100 North Glebe Road, Arlington, VA 22201	2. Year Firm Established: 1962	3. Date Prepared: June 27, 2012
4. Type of Firm: __A. Small Business __B. Small Disadvantaged __C. Woman-Owned __D. Hubzone __E. Service-Disabled Veteran-Owned _X_ F. Other (Specify) Large		
5. Principal Points of Contact: (List two by Name/Title/Current Telephone Number) Greg Scovel, Vice President, 703-679-3295 Rachel Mayhew, Contracts Administrator, 703-679-3321		
6. Present Offices: (Address/Telephone) – Over 150 offices worldwide, mostly in the DC Metro area HQ: 1100 North Glebe Road, Arlington, VA 22201, 703-841-7800		
7. Past Performance Last 3 Years (1) List Contracts Similar in Size (Dollars) and Scope; (2) List Contracts Similar in Scope Only		
Contract No: N00178-04 – D-4026, V701 Period of Performance: Mar 2008 – Mar 2013 Dollar Value: $44M Name of Gov./Commercial Entity: Department of Commerce	Contracting Contact Name & Phone: Mr. Kim Bryant – 843-218-4143 Technical Rep. Name & Phone: Mr. Kim Bryant – 843-218-4143	Brief Description and How it is Similar to NRC's Requirement: Designed, built and currently operate the DOC/BIS Security Operations Center. Included analysis of best practices, new technologies and business solutions.
Contract No: GS07T00BGD0021 Period of Performance: Oct 2006 – Sept 2011 Dollar Value: $93M Name of Gov./Commercial Entity: Office of Secretary of Defense/CIO	Contracting Contact Name & Phone: Duane Parsons, 703-696-0427 Technical Rep. Name & Phone: Rusty Bowling, 703-695-6696	Brief Description and How it is Similar to NRC's Requirement: Performed Risk management, C&A, incident response, security training, FISMA compliance, analysis of best practices, new technologies and business solutions.
Contract No: W15P7T06DE402 TO 114 Period of Performance: Mar 2011 – Apr 2012 Dollar Value: $41M Name of Gov./Commercial Entity: US Army CECOM LCMC	Contracting Contact Name & Phone: David Greaves, 443-861-4647 Technical Rep. Name & Phone: Kevin Ha, 443-395-5715	Brief Description and How it is Similar to NRC's Requirements: IA Engineering practices similar to Enterprise Security Architecture. Assessing the system development lifecycle for efficiencies in achieving security and

The foregoing is a statement of facts

Signature: Rachel F. Mayhew Title: Contracts Administrator Date: 6-22-2012

1. Firm Name & Address: **Knowledge Consulting Group, Inc.,** 11710 Plaza America Drive, Suite 520, Reston, VA 20190	2. Year Firm Established: 2000	3. Date Prepared: June 27, 2012
4. Type of Firm: X A. Small Business __B. Small Disadvantaged __C. Woman-Owned __D. Hubzone __E. Service-Disabled Veteran-Owned __F. Other (Specify)_____		
5. Principal Points of Contact: (List two by Name/Title/Current Telephone Number) Sherrie Nutzman: Director, Finance & Administration – tel 703.467.2000 x 103 J.G. Meyer: Vice President, Operations – tel 703.467.2000 x 121		
6. Present Offices: (Address/Telephone) Knowledge Consulting Group, Inc., 11710 Plaza America Drive, Suite 520, Reston, VA 20190, 703-467-2000		
7. Past Performance Last 3 Years (1) List Contracts Similar in Size (Dollars) and Scope; (2) List Contracts Similar in Scope Only		
Contract No: IDIQ HSTS03-11-D-CIO556 Period of Performance: 08/02/2011 – 08/01/2016 Dollar Value: Ceiling $190M Name of Gov./Commercial Entity: Transportation Security Administration (TSA)	Contracting Contact Name & Phone: Kristin Fuller, Branch Chief, Infrastructure Division, Contracting Officer Phone Number: (571) 227-2740 Technical Rep. Name & Phone: Jill Vaughan, Phone Number: (571) 227-2034	Brief Description and How it is Similar to NRC's Requirement: Please see below.
Description: KCG is the prime contractor providing over 50 credentialed and cleared information security services professionals in support of TSA OIT and other Program Offices within TSA spanning 14 separate task orders. KCG security professionals provide ISSO, Certification and Accreditation, IV&V, FISMA compliance, IT Training and Awareness, IT Security Architecture, Security Policy, Digital Forensics, E-Discovery, SOC Management, COMSEC, and Cyber Critical Infrastructure and Planning services to TSA as their primary IA prime contractor. **Directly relevant to the CSPSS SOW**: KCG's support to TSA is directly relevant to the NRC requirements. KCG is responsible for maintaining and managing TSA's FISMA inventory and is responsible for developing and reviewing all authorization packages. KCG is responsible for providing cyber situational awareness by providing vulnerability assessment services, performing incident response, maintaining the Digital Forensics Lab, TSA's technical standards and security architecture, and evaluating the security designs and configurations of all TSA systems. KCG provides security policy support to the policy team within IAD and is responsible for developing and maintaining TSA's policy handbook, technical standards, policy guidance presentations, waivers and exception program, and standard operating procedures.		

Contract No: GS-35F-0448N, Delivery Order HSCETC-08-F-00033 Period of Performance: 9/30/08 – 10/01/12 Dollar Value: $10.8M (ongoing) Name of Gov./Commercial Entity: Department of Homeland Security (DHS), Immigration and Customs Enforcement (ICE)	Contracting Contact Name & Phone: Ben Branch Phone Number: (202) 732-2669 Technical Rep. Name & Phone: Scott Townsend, COTR Phone Number: (202) 732-7207	Brief Description and How it is Similar to NRC's Requirement: Please see below.

Description: KCG is the prime contractor for ICE's Information Assurance Directorate (IAD) providing comprehensive information security support services under the Security Management Oversight and Compliance (SMOC) contract. KCG is responsible for developing, implementing, and managing ICE's enterprise ISSO program under the SMOC contract providing ISSO support to all major ICE program areas. Within IAD, KCG provides Security Authorization and Risk Management support, security awareness and training, security engineering, ICAM, security policy, security architecture, and overall governance support. KCG manages ICE's entire FISMA inventory of over 90 systems including 10 separate GSS'. KCG's ISSOs are responsible for developing all appropriate Authorization artifacts including SSPs, CPs, SARs, POA&Ms, and Authorization recommendations utilizing RMS and Trusted Agent FISMA. Our team makes recommendations on security process improvements, manages the SA&A program and serves in numerous trusted-advisor roles. During our support of ICE, FISMA scores have risen 25% overall, and we performed a top-down information security training review improving the skill set of each support ISSO. Since KCG has served as the prime contractor, ICE has received an A FISMA score.

Directly relevant to the CSPSS SOW: KCG's support to ICE is directly relevant to the NRC requirements. KCG is responsible for developing and reviewing authorization packages for ICE's entire FISMA inventory of 90+ systems. KCG's ISSOs develop all authorization packages, provide log analysis, and review scan results for their assigned system. KCG's Risk Analysts review all authorization packages for content and validity prior to submitting to the Authorizing Official along with a risk recommendation. KCG's Governance professionals are responsible for developing and maintaining ICE security policies. For each policy developed, KCG develops a policy handbook to provide further explanation for ensuring compliance with the policy.

Contract No: GS-35F-0448N Period of Performance: 9/30/2009 – 9/30/2014 Dollar Value: $6.5M Name of Gov./Commercial Entity: Department of Education, Federal Student Aid (FSA)	Contracting Contact Name & Phone: Richard Segich Phone Number: 202.377.3918 Technical Rep. Name & Phone: Robert Ingwalson Phone Number: 202.377.3463	Brief Description and How it is Similar to NRC's Requirement: Please see below.

Description: KCG is providing direct support for Federal Student Aid's Chief Information Security Officer as a part of their Security & Privacy Team. KCG provides Information Security Program Management Support, Information Assurance Support (e.g., C&A, Security Authorization), Information Security Governance Support, and Vulnerability Assessment support.

Directly relevant to the CSPSS SOW: KCG's team of IA specialists are responsible for ensuring all FSA systems maintain and obtain Authority to Operate for over 30 systems and for facilitating the collection and reporting of FISMA metrics on a quarterly and annual basis. Our team led the adoption of the Security Authorization approach in alignment with the NIST Risk Management Framework. Additionally, KCG has established a Continuous Security Authorization (CSA) program for Federal Student Aid whereby the security posture for all FISMA reportable systems are validated on a frequent schedule (quarterly) based on operating risk. In support of FSA initiatives, KCG has developed policy documents and requirements for operating the security authorization and CSA programs. This includes coordination of internal FSA resources and reporting frequency to decision makers. As part of the security authorizations and CSA, KCG generates discovered deficiencies in the form of Plan of Action and Milestones (POAMs). All POAMs are documented based on NIST SP 800 series recommendations and guidelines.

The foregoing is a statement of facts

Signature: _____ Title: Vice President, Operations Date: June 27, 2012

1. Firm Name & Address: **Prometheus Global, Inc.,** 14121 Parke-Long Dr. Suite 220, Chantilly, VA 20191	2. Year Firm Established: 2003	3. Date Prepared: June 27, 2012
4. Type of Firm: X A. Small Business __B. Small Disadvantaged __C. Woman-Owned __D. Hubzone __E. Service-Disabled Veteran-Owned __F. Other (Specify)_____		
5. Principal Points of Contact: (List two by Name/Title/Current Telephone Number) Michael Shinn, CEO 703-266-6006 x101, 703-403-6935 (cell) Casey Priester, Vice President 703-266-6006 x103, 703-725-9538 (cell)		
6. Present Offices: (Address/Telephone) 14121 Parke-Long Dr. Suite 220, Chantilly, VA 20191		
7. Past Performance Last 3 Years (1) List Contracts Similar in Size (Dollars) and Scope; (2) List Contracts Similar in Scope Only		
Contract No: W15P7T-06-D-E402 / S3R-0475 Period of Performance: 10/11 – 9/13 Dollar Value: $1,786,001.46 Name of Gov./Commercial Entity: U.S. Army REDCOM, CERDEC, I2WD QRC Branch	Contracting Contact Name & Phone: Geoffrey Hermansdorfer (410) 553-3435 Technical Rep. Name & Phone: Adam Bogner QRC Branch Chief	Brief Description and How it is Similar to NRC's Requirement: Certification and Accreditation under DIACAP and CENTCOM C&A requirements. Provide Information Assurance (IA) Support for identification and resolution of Information Assurance issues and concerns. Develop and contribute to guidelines, plans, policies, analyses and reviews that require IA expertise in the areas of System Security Authorization Agreement (SSAA) Assessments, Review and Processing Initial Authority to Operate (IATO), Accreditation, Certification, Port Protocol and Services (PPS) evaluation, Chief Information Office (CIO) Assessments.

Contract No: GS-35F-0306J/HHM402-04-A-0010/0059 Period of Performance: 11/09 – 11/10 Dollar Value: $150,462.40 Name of Gov./Commercial Entity: Defense Intelligence Agency, Information Assurance Protection Center	Contracting Contact Name & Phone: Jon C. Perry 703-984-3352 Technical Rep. Name & Phone: Terrence Maddeaux 202-231-4454	Brief Description and How it is Similar to NRC's Requirement: Security O&M, Continuous Monitoring, and Incident Response duties. Preparation of ConOps. Member of Change Advisory Board. Security oversight for multiple network enclaves, web applications, and customized software. Preparation and delivery of SSAAs, ConOps, and related security program deliverables related to SSDLC
Contract No: PO 5660018282, "FTK Enterprise Forensics Lab" Period of Performance: 8/11 – 12/11 Dollar Value: $71,176 Name of Gov./Commercial Entity: Sempra Energy	Contracting Contact Name & Phone: Scott King 858-613-5716 Technical Rep. Name & Phone: Scott King 858-613-5716	Brief Description and How it is Similar to NRC's Requirements: Perform complete INFOSEC Assessment of implementation of secure forensics lab. Provide SME-level guidance on IA-related issues. Provide input into secure build standards and operating procedures. Perform penetration testing on lab for quality assurance purposes.

The foregoing is a statement of facts

Signature: Casey Prieste Title: Vice President Date: 06/27/2012

4.2 Awards, Accolades, and Letters of Commendation

RFP Section E.9, page E-6

MAR, Incorporated was awarded ISO 9001:2008 certification according to International Quality Registrars (IQR) on June 13, 2011. In addition, MAR passed its first sixth month surveillance in January 2012. Four of MAR's management team completed the ISO 9001:2008 Internal Auditor Program and are hereby certified to perform ISO internal audits.

From: Welkie, Andrew
Subject: RE: DDMS Findings Tracking sheet for annual hardening requirement
Sent: Thursday, April 19, 2012 2:02 PM
"Thanks and it has been a pleasure working with MAR the past several years!"
Andy

From: Natalya Bobryakova
Subject: FW: Draft IRSD scorecard
Sent: Monday, April 02, 2012 4:29 PM
"Thank you for your great support!"
Natalya Bobrykova

From: Brosky, Kathleen
Subject: RE: Delivery: FAIMIS Test Environment Findings Tracking Sheet
Sent: Friday, March 16, 2012 9:34 AM
"Thanks to all you for getting this delivered to us ahead of schedule".
Kathleen

From: Peyton, James
Subject: RE: Delivery: ACS Contingency Plan and Contingency Test Report
Sent: Monday, March 05, 2012 11:41:24 AM
"I was very pleased with the execution of the CP test and am glad that Contingency Test Report is overwhelmingly positive".
Jim Peyton

From: Flynn, Sean
Subject: RE: Summary of phone call for Region II SSP/BIA/CP updates
Sent: Thursday, January 12, 2012 12:57 PM
"Thanks. I very much appreciate your assistance and professionalism".
Sean

From: Sage, Alan
Subject: RE: Request for Extension of Authority to Operate (ATO) for the Emergency Response Data System (ERDS)
Sent: Wednesday, November 02, 2011 8:52 AM
"... Excellent job."
Alan

From: Peyton, James
Subject: RE: Status of ASCT for SLES
Sent: Tuesday, February 14, 2012 2:39 PM
"Excellent, thank you. .... Thanks for being so responsive!"
Jim

From: Natalya Bobryakova
Subject: RE: Delivery: Draft ADAMS SRA and SSP Updates
Sent: Monday, July 11, 2011 10:34 AM
"Thank you all very much! I really appreciate both the quality and timeliness of these deliverables".
- Natalya

From: Steve Liu
Subject: Thanks: SFST Classified Laptop
Sent: Tuesday, October 25, 2011 4:03 PM
"Bill and Tom, Thanks to Brian's outstanding work, the scan/harden on NMSS/SFST classified laptop was completed today. The job is well done. We have struggled to find a solution for this task a long time. I am so glad that CSO and MAR help us to get through this. Brain is a great asset to NRC IT security world. He completed the work so quickly. Excellent! Thank you all. Steve"

From: Natalya Bobryakova
Subject: RE: Delivery: Final Public ADAMS Web Applications VAR
Sent: Thursday, August 11, 2011 2:22 PM
"I want to thank the MAR team for a great job they did in a two-phase security testing of the ADAMS Public Web applications. Thanks to them, we resolved a critical vulnerability before starting the User Acceptance Testing. Also, I am really thankful to Bill Dabbs and Thorne Graham for providing the technical guidance. It was a good teamwork! Thanks again, Natalya Bobryakova"

From: Lovell, Louise
Subject: Letter of Appreciation
Sent: Friday, January 29, 2010 5:02 PM
"Tom, I greatly appreciate the outstanding support that Mr. John Ribeiro of your technical staff has provided for the mitigation and resolution of the POAMs for the OCIMS Project. These identified security risks had resulted in a highly visible risk profile for this investment which is mission critical for the agency. Many of these were broadly defined and required updates to security documentation and enhanced procedures to address the auditing and oversight controls. NIST guidelines called for increased procedures in System Administration and management of User Accounts to protect and track system access. John has handled our needs for additional security controls with knowledge, professionalism, and timeliness. He has brought technical depth to the security scanning and patching for the servers. In addition, he has been proactive in defining realistic enhancements to existing procedures and interfacing with our Computer Security Office in clarifying areas that should be addressed by waivers from the controls. This is particularly significant for the Security Event Logging capability which is more cost effectively implemented as an agency wide implementation which would include the OCIMS logging. I have also appreciated his readiness to work with the OCIMS technical staff to clarify and implement required changes. John has followed up on questions and issues; and provided excellent customer service and a high quality of expertise in security control concepts and implementations. He has supported staff with varying technical backgrounds and responsibilities. Many thanks to MAR for providing outstanding technical staff such as Mr. John Riberio. His work has resulted in the significant cleanup and resolution of OCIMS POAMS. We look forward to his expertise in the on-going quarterly security scanning and reporting that is now underway to maintain the security posture for this mission-critical system. Louise"

From: Lovell, Louise
Subject: Letter of Appreciation
Sent: Thursday, December 03, 2009 6:25 PM
"MAR Management. I greatly appreciate the support that Mr. Tom Evans, MAR Task Order Project Manager, provided for the NSIR SGI Laptop Certification and Accreditation during 2009. I have been the NSIR Project Manager and responsible for ensuring that our office laptops are in compliance with new Computer Security Office policies and procedures for laptop certification. MAR's activities included development of the certification package, application of security patches, changes in configuration settings, and establishing new monitoring practices. Tom planned the MAR task work and led his Technical Staff through the steps that were required for this effort. Because some of these procedures were new, Tom's work also involved creativity and flexibility in adjusting work to the new requirements. Following are examples of Tom's leadership in accomplishing our certification tasks:

- *clarifying new CSO security procedures and requirements*
- *quickly adjusting technical staffing to ensure appropriate experience and skills*
- *working with CSO to develop and pilot security certification processes*
- *working with CSO to develop continuous scanning and patching processes that will be needed for maintaining adequate security controls*

Tom has handled our discussions and meetings with knowledge, professionalism, timeliness, and an appreciation for tradeoffs between risk, investment, and agency priorities. He has been proactive and brought technical depth to refining the certification checklists, configurations, security procedures and reporting. He has followed up on questions and issues and provided a high level of responsiveness in clarifying task work. Tom's efforts contributed significantly to moving our certification ahead and resulted in our achieving the Authorization to Operate for these laptops early this week. Louise Lovell, NSIR Project Manager "

From: Louise Lovell
Subject: Letter of Appreciation
Sent: Monday, August 24, 2009 6:01 PM
"Tom, I greatly appreciate the outstanding support that Mr. Brian Pham of your technical staff has provided for the certification and accreditation of the specialized office laptops. These laptops have required special configurations and security controls to protect sensitive information which is processed by them. The System Administration and User Accounts have required additional procedures and controls to protect and track access. Brian has handled our requirements with knowledge, professionalism, and timeliness. He has brought technical depth to the security scanning and patching for the individual laptops. In addition, he has been proactive in developing new procedures and interfacing with our Computer Security Office in implementing new agency policy and guidance in our environment. I have also appreciated his readiness to work with the technical staff in the Office of Information Services in developing a standard image that may be supported agency wide. Brian has followed up on questions and issues; and provided excellent customer service and a high quality of support and responsiveness to a variety of staff with varying technical backgrounds and responsibilities. Many thanks to MAR for providing outstanding technical staff such as Mr. Brian Pham. His work has resulted in the timely completion of the certification package for these laptops which are critical to office business functions. Louise Lovell"

From: David Curtis
Sent: August 30, 2007, 11:25 AM
"Audrey, I have had an opportunity to review the document and I wanted to thank you and your team for your work. I am pleased with the quality of the work and the attention to detail.

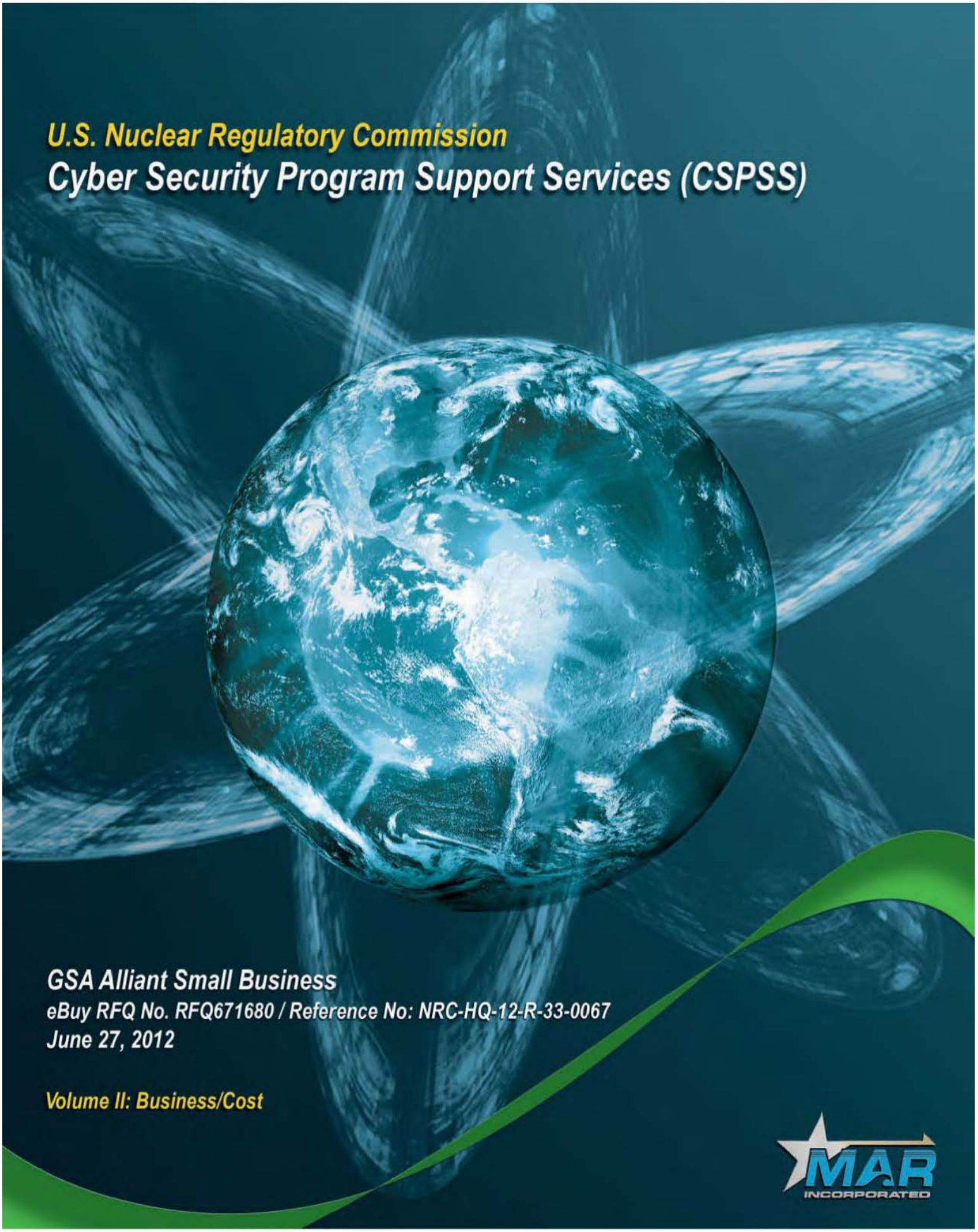
Working with Ericka has been very pleasurable, and she politely kept me moving to get the document completed. I have forwarded the SecCat to the system owner for his final review, and expect it to be forwarded to the SITSO shortly. David"

From: Karen Paradiso
Subject: Fwd: System Self Assessments
Sent: August 15, 2007
"Hi Charlie, I have reviewed the System Self Assessments and provided you with the sign-off form. I do have a few comments. First, as I indicated previously I appreciate MAR documenting the system assessments. With the information that they were provided and the short-turnaround they did a good job. However, I did notice that in attempting to document the inherited controls they did not have quite enough information to document these accurately for each system. Some things don't inherit quite as cleanly as we would like for each system!! Actually, it's my job then to make sure the documentation is accurate!! Based on that, I did not get to finish updating each document to be as accurate as I would like. Attached are the updated versions for LAN/WAN, DCS and MPKI. Web Servers is based on last years...I'm OK with that as well. I will update the others as best I can next week...in between POAMs and E300!! Thanks! Karen"

4.3 List of Terminated Contracts

RFP Section E.9, page E-6

MAR, Incorporated has not had any contracts terminated for default or for cause. MAR has not received any show cause letters, cure notices, or poor performance letters.



U.S. Nuclear Regulatory Commission
Cyber Security Program Support Services (CSPSS)

GSA Alliant Small Business
eBuy RFQ No. RFQ671680 / Reference No: NRC-HQ-12-R-33-0067
June 27, 2012

Volume II: Business/Cost

MAR INCORPORATED

VOLUME II
BUSINESS/COST

RESPONSE TO:
RFQ NO.: 671680
REFERENCE NO.: NRC-HQ-12-R-33-0067
CYBER SECURITY PROGRAM SUPPORT SERVICES (CSPSS)

27 JUNE 2012

PREPARED FOR:
Nuclear Regulatory Commission
(NRC)

DELIVERED TO:
Jordan.pulaski@nrc.gov
Joseph.widdup@nrc.gov

ATTENTION:
Jordan Pulaski, Senior Contract Specialist
Joseph Widdup, Contracting Officer

SUBMITTED BY:
MAR, INCORPORATED
1803 Research Blvd, Suite 204, Rockville, MD 20850-6106

MAR PROPOSAL NUMBER: 2012-080/WA1685

This response includes data that is furnished in connection with RFQ No. 671680 and MAR Proposal Number 2012-080/WA1685 and shall not be disclosed outside the Government and shall not be duplicated, used, or disclosed – in whole or in part – for any purpose other than to evaluate this proposal. If, however, a contract is awarded to this offer or as a result of – or in connection with – the submission of this data, the Government shall have the right to duplicate, use, or disclose the data to the extent provided in the resulting contract. This restriction does not limit the Government's right to use information contained in this data if it is obtained from another source without restriction. The data subject to this restriction are contained in MAR Proposal Number 2012-080/WA1685.

Table of Contents

INTRODUCTION 1
1.0 ACKNOWLEDGEMENT OF SOLICITATION AND AMENDMENTS 2
1.1 Standard Form 1449 2
1.1 Standard Form 30 – Amendments 1, 2, and 3 3
2.0 PURCHASING SYSTEM ACCEPTANCE/APPROVAL 7
3.0 RFP PROVISIONS E.1 AND E.4 8
3.1 MAR, Incorporated's Response to RFP Provisions E.1 and E.4 8
3.1.1 MAR, Incorporated's Response to RFP Provision E.1 2052.209-71 Contractor Organizational Conflicts Of Interest (Representation) (Oct 1999) 8
3.1.2 MAR, Incorporated's Response to RFP Provision E.4 2052.209-70 Current/Former Agency Employee Involvement (Oct 1999) 9
3.2 MAR, Incorporated's Subcontractors' Response to RFP Provisions E.1 and E.4 10
3.2.1 CACI's Response to RFP Provisions E.1 and E.4 10
3.2.2 Convergent's Response to RFP Provisions E.1 and E.4 12
3.2.3 DCCA's Response to RFP Provisions E.1 and E.4 14
3.2.4 Knowledge Consulting Group's Response to RFP Provisions E.1 and E.4 16
3.2.5 Mainstay's Response to RFP Provisions E.1 and E.4 18
3.2.6 Prometheus Global's Response to RFP Provisions E.1 and E.4 20
3.2.7 Securicon's Response to RFP Provisions E.1 and E.4 22
4.0 COST/PRICE 24
4.1 CSPSS Base Period Cost/Price 28
4.1.1 CSPSS Base Period Cost/Price – Part 1 28
4.1.2 CSPSS Base Period Cost/Price – Part 2 29
4.1.3 CSPSS Base Period Cost/Price – Part 3 30
4.1.4 CSPSS Base Period Cost/Price – Part 4 31
4.1.5 CSPSS Base Period Cost/Price – Part 5 32
4.2 CSPSS Option 1 Cost/Price 33
4.2.1 CSPSS Option 1 Cost/Price – Part 1 33
4.2.2 CSPSS Option 1 Cost/Price – Part 2 34
4.2.3 CSPSS Option 1 Cost/Price – Part 3 35
4.2.4 CSPSS Option 1 Cost/Price – Part 4 36
4.2.5 CSPSS Option 1 Cost/Price – Part 5 37
4.3 CSPSS Option 2 Cost/Price 38
4.3.1 CSPSS Option 2 Cost/Price – Part 1 38
4.3.2 CSPSS Option 2 Cost/Price – Part 2 39
4.3.3 CSPSS Option 2 Cost/Price – Part 3 40
4.3.4 CSPSS Option 2 Cost/Price – Part 4 41
4.3.5 CSPSS Option 2 Cost/Price – Part 5 42
4.4 CSPSS Option 3 Cost/Price 43
4.4.1 CSPSS Option 3 Cost/Price – Part 1 43
4.4.2 CSPSS Option 3 Cost/Price – Part 2 44
4.4.3 CSPSS Option 3 Cost/Price – Part 3 45
4.4.4 CSPSS Option 3 Cost/Price – Part 4 46
4.4.5 CSPSS Option 3 Cost/Price – Part 5 47

Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this proposal.

4.5 CSPSS Option 4 Cost/Price 48
4.5.1 CSPSS Option 4 Cost/Price – Part 1 ..... *48*
4.5.2 CSPSS Option 4 Cost/Price – Part 2 ..... *49*
4.5.3 CSPSS Option 4 Cost/Price – Part 3 ..... *50*
4.5.4 CSPSS Option 4 Cost/Price – Part 4 ..... *51*
4.5.5 CSPSS Option 4 Cost/Price – Part 5 ..... *52*
4.6 CSPSS Option 5 Cost/Price 53
4.6.1 CSPSS Option 5 Cost/Price – Part 1 ..... *53*
4.6.2 CSPSS Option 5 Cost/Price – Part 2 ..... *54*
4.6.3 CSPSS Option 5 Cost/Price – Part 3 ..... *55*
4.6.4 CSPSS Option 5 Cost/Price – Part 4 ..... *56*
4.6.5 CSPSS Option 5 Cost/Price – Part 5 ..... *57*
4.7 CSPSS Option 6 Cost/Price 58
4.7.1 CSPSS Option 6 Cost/Price – Part 1 ..... *58*
4.7.2 CSPSS Option 6 Cost/Price – Part 2 ..... *59*
4.7.3 CSPSS Option 6 Cost/Price – Part 3 ..... *60*
4.7.4 CSPSS Option 6 Cost/Price – Part 4 ..... *61*
4.7.5 CSPSS Option 6 Cost/Price – Part 5 ..... *62*
4.8 CSPSS Option 7 Cost/Price 63
4.8.1 CSPSS Option 7 Cost/Price – Part 1 ..... *63*
4.8.2 CSPSS Option 7 Cost/Price – Part 2 ..... *64*
4.8.3 CSPSS Option 7 Cost/Price – Part 3 ..... *65*
4.8.4 CSPSS Option 7 Cost/Price – Part 4 ..... *66*
4.8.5 CSPSS Option 7 Cost/Price – Part 5 ..... *67*
4.9 CSPSS Option 8 (3 Months) Cost/Price 68
4.9.1 CSPSS Option 8 Cost/Price – Part 1 ..... *68*
4.9.2 CSPSS Option 8 Cost/Price – Part 2 ..... *69*
4.9.3 CSPSS Option 8 Cost/Price – Part 3 ..... *70*
4.9.4 CSPSS Option 8 Cost/Price – Part 4 ..... *71*
4.9.5 CSPSS Option 8 Cost/Price – Part 5 ..... *72*
4.10 CSPSS Cost/Price Summary for Base and Options 73
ATTACHMENT 1 – MAR, INCORPORATED'S GSA ALLIANT SMALL BUSINESS CONTRACT WITH MODIFICATIONS A-1

List of Tables

Table 1. MAR Proposed Labor Categories and Discounted Hourly Rates 24

Description of Acronyms and Abbreviations

Acronym	Description
CISSS	Consolidated Information System Security Services
CLIN	Contract Line Item Number
CNSS	Committee on National Security Systems
CSO	Computer Security Office
CSPSS	Cyber Security Program Support Services
FFP	Firm–Fixed-Price
FIPS	Federal Information Processing Standards
GAO	Government Accountability Office
GSA ASB	General Services Administration Alliant Small Business
HQ	Headquarters
MAR	MAR Incorporated
NIST	National Institute of Standards and Technology
NRC	Nuclear Regulatory Commission
OCOI	Organizational Conflict of Interests
ODC	Other Direct Cost(s)
OMB	Office of Management and Budget
PMOS	Program Management Oversight System
RFP	Request for Proposal
SOW	Statement of Work
T&M	Time-and-Materials

INTRODUCTION

MAR's cost proposal was developed from our team's combined Cyber Security experience along with the performance metrics captured in our TaskTracker system used to support the NRC CISSS contract. Starting with historical trends as a basis we developed a realistic mix of labor hours and resource distribution for each of Attachment D's unit and ceiling price CLINS.

MAR, Incorporated (MAR) is pleased to provide the NRC this Business/Cost Proposal in response to NRC-HQ-12-R-33-0067. Our proposal is fully responsive to Section E.9 of the RFP. We believe it is clear, accurate, and reflects a realistic cost approach to efficiently completing the tasks for CSPSS.

HIGHLIGHTS

- *MAR and our subcontractors have certified we are clear of any NRC OCOI for the past three years.*
- *MAR's cost proposal was developed using NRC CISSS metrics as a starting baseline.*
- *We have prepared realistic unit pricing through aggressive labor rate discounting and a balanced labor mix.*

Under the NRC General Services Administration Alliant Small Business (GSA ASB) task order MAR will deliver firm-fixed-price (FFP) and time-and-materials (T&M) services as outlined in the Statement of Work (SOW) and in accordance with the cost model requested in Attachment D of the RFQ. MAR is not proposing any fixed hourly labor rates that exceed the Year 4 fixed hourly rates in our current GSA ASB contract. We have selected specific labor categories and have significantly discounted the associated rates to deliver the services required under this project. Our proposal was prepared based on the understanding the NRC will add the total proposed cost/price for each option period to the total cost/price for the base period to determine the total proposed cost/price. It is understood that the NRC may perform cost realism analysis to derive an evaluated cost/price for each contract year and for the entire proposal.

Within this volume we have included:

- Acknowledgment of the receipt of the solicitation and amendments as posted on GSA eBuy under the GSA ASB.
- Documentation of MAR's purchasing system acceptance/approval.
- Response to RFP Provision E.1 2052.209-71 Contractor Organizational Conflicts Of Interest (OCOI) along with documented certification of no OCOI issues for MAR and each of our proposed subcontractors.
- Response to RFP Provision E.4 2052.209-70 Current/Former Agency Employee Involvement for MAR and each of our proposed subcontractors.
- The Cost/Price narrative, proposed GSA ASB labor categories, discounted rates, and base and option year pricing.
- A copy of the MAR GSA ASB contract with all modifications.

Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this proposal.

1.0 ACKNOWLEDGEMENT OF SOLICITATION AND AMENDMENTS

RFP Section E.9, page 5

1.1 Standard Form 1449

RFP Section E.9, page 5

SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS
OFFEROR TO COMPLETE BLOCKS 12, 17, 23, 24, & 30

1. REQUISITION NO. | PAGE 1 OF XX

2. CONTRACT NO.	3. AWARD/EFFECTIVE DATE	4. ORDER NO.	5. SOLICITATION NUMBER	6. SOLICITATION ISSUE DATE
			NRC-HQ-12-R-33-0067	May 2, 2012

7. FOR SOLICITATION INFORMATION CALL:	a. NAME	b. TELEPHONE NO. (No Collect Calls)	8. OFFER DUE DATE/LOCAL TIME
			June 15, 2012 4:00 P.M. EST

9. ISSUED BY — CODE 3150
U.S. Nuclear Regulatory Commission
Div. of Contracts
Attn: Jordan Bulaski
Mail Stop: TWB-01-B10M
Washington, DC 20555

10. THIS ACQUISITION IS
- [ ] UNRESTRICTED OR [X] SET ASIDE: 100 % FOR:
- [X] SMALL BUSINESS
- [ ] WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOMEN-OWNED SMALL BUSINESS PROGRAM
- [ ] HUBZONE SMALL BUSINESS
- [ ] EDWOSB
- [ ] SERVICE DISABLED VETERAN-OWNED SMALL BUSINESS
- [ ] 8(A)

NAICS: 541519
SIZE STANDARD: $25.5 Million

11. DELIVERY FOR FOB DESTINATION UNLESS BLOCK IS MARKED	12. DISCOUNT TERMS	13a. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)	13b. RATING	14. METHOD OF SOLICITATION
[ ] SEE SCHEDULE	N/A	[ ]	N/A	[ ] RFQ [ ] IFB [X] RFP

15. DELIVER TO — CODE
U.S. Nuclear Regulatory Commission

Washington DC 20555

16. ADMINISTERED BY — CODE 3100
U.S. Nuclear Regulatory Commission
Div. of Contracts
Mail Stop: TWB-01-B10M

Washington, DC 20555

17a. CONTRACTOR/OFFEROR CODE | FACILITY CODE

MAR, Incorporated
1803 Research Boulevard, Suite 204
Rockville, MD 20850

TELEPHONE NO. 301-231-0100

18a. PAYMENT WILL BE MADE BY — CODE 3100
Department of Interior / NBC
NRCPayments_NBCDenver@NBC.gov
Attn: Fiscal Services Branch - D2770
7301 W. Mansfield Avenue
Denver CO 80235-2230

PHONE: FAX:

[ ] 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
[ ] SEE ADDENDUM

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	The contractor shall provide the U.S. Nuclear Regulatory Commission (NRC) with the services described in the enclosed Statement of Work (SOW) - Attachment A, and terms and conditions of this task order.				

(Use Reverse and/or Attach Additional Sheets as Necessary)

25. ACCOUNTING AND APPROPRIATION DATA

26. TOTAL AWARD AMOUNT (For Govt. Use Only)

[X] 27a. SOLICITATION INCORPORATES BY REFERENCE FAR 52.212-1, 52.212-4. FAR 52.212-3 AND 52.212-5 ARE ATTACHED. ADDENDA [X] ARE [ ] ARE NOT ATTACHED

[ ] 27b. CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4. FAR 52.212-5 IS ATTACHED. ADDENDA [ ] ARE [ ] ARE NOT ATTACHED

[ ] 28. CONTRACTOR IS REQUIRED TO SIGN THIS DOCUMENT AND RETURN ____ 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.

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)	
30b. NAME AND TITLE OF SIGNER (TYPE OR PRINT): Michael P. Norcio, Chairman and Chief Executive Officer	30c. DATE SIGNED: June 27, 2012	31b. NAME OF CONTRACTING OFFICER (TYPE OR PRINT): Joseph L. Widdup, Contracting Officer	31c. DATE SIGNED

AUTHORIZED FOR LOCAL REPRODUCTION
PREVIOUS EDITION IS NOT USABLE

STANDARD FORM 1449 (REV. 2/2012)
Prescribed by GSA - FAR (48 CFR) 53.212

1.1 Standard Form 30 – Amendments 1, 2, and 3

RFP Section E.9, page 5

AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT

BPA NO.	1. CONTRACT ID CODE	PAGE	OF PAGES
		1	1

2. AMENDMENT/MODIFICATION NO.	3. EFFECTIVE DATE	4. REQUISITION/PURCHASE REQ. NO.	5. PROJECT NO. (If applicable)
1		NRC-HQ-R-33-0067	

6. ISSUED BY CODE 3100

U.S. Nuclear Regulatory Commission
Div. of Contracts
Attn: Jordan Pulaski
Mail Stop: TWB-01-B10M
Washington, DC 20555

7. ADMINISTERED BY (If other than Item 6) CODE 3100

U.S. Nuclear Regulatory Commission
Div. of Contracts
Mail Stop: TWB-01-B10M

Washington, DC 20555

8. NAME AND ADDRESS OF CONTRACTOR (No., street, county, State and ZIP Code)

To all Offerors/Bidders
MAR, Incorporated
1803 Research Boulevard, Suite 204
Rockville, MD 20850

(X) 9A. AMENDMENT OF SOLICITATION NO.
NRC-HQ-12-R-33-0067

9B. DATED (SEE ITEM 11)
X 06-01-2012

10A. MODIFICATION OF CONTRACT/ORDER NO.

10B. DATED (SEE ITEM 13)

CODE FACILITY CODE

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

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

12. ACCOUNTING AND APPROPRIATION DATA (If required)

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

(X) A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: (Specify authority) THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NO. IN ITEM 10A.

B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES (such as changes in paying office, appropriation date, etc.) SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(b).

C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF:

D. OTHER (Specify type of modification and authority)

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

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

Please see the attached responses to questions.

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

15A. NAME AND TITLE OF SIGNER (Type or print)	16A. NAME AND TITLE OF CONTRACTING OFFICER (Type or print)
Michael P. Norcio Chairman and Chief Executive Officer	Joseph Widdup
15B. CONTRACTOR/OFFEROR (Signature of person authorized to sign)	15C. DATE SIGNED June 27, 2012
16B. UNITED STATES OF AMERICA BY (Signature of Contracting Officer)	16C. DATE SIGNED

NSN 7540-01-152-8070
PREVIOUS EDITION NOT USABLE

STANDARD FORM 30 (REV. 10-83)
Prescribed by GSA - FAR (48 CFR) 53.243

AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT	BPA NO.	1. CONTRACT ID CODE	PAGE 1	OF PAGES 1

2. AMENDMENT/MODIFICATION NO.	3. EFFECTIVE DATE	4. REQUISITION/PURCHASE REQ. NO.	5. PROJECT NO. (If applicable)
A002		NRC-HQ-R-33-0067	

6. ISSUED BY	CODE 3100	7. ADMINISTERED BY (If other than Item 6)	CODE 3100
U.S. Nuclear Regulatory Commission Div. of Contracts Attn: Jordan Pulaski Mail Stop: TWB-01-B10M Washington, DC 20555		U.S. Nuclear Regulatory Commission Div. of Contracts Mail Stop: TWB-01-B10M Washington, DC 20555	

8. NAME AND ADDRESS OF CONTRACTOR (No., street, county, State and ZIP Code)

To all Offerors/Bidders

MAR, Incorporated
1803 Research Boulevard, Suite 204
Rockville, MD 20850

(X) 9A. AMENDMENT OF SOLICITATION NO.
NRC-HQ-12-R-33-0067

9B. DATED (SEE ITEM 11)
X 06-05-2012

10A. MODIFICATION OF CONTRACT/ORDER NO.

10B. DATED (SEE ITEM 13)

CODE FACILITY CODE

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

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

12. ACCOUNTING AND APPROPRIATION DATA (If required) N/A.

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

(X) A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: (Specify authority) THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NO. IN ITEM 10A.

B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES (such as changes in paying office, appropriation date, etc.) SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(b).

C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF:

D. OTHER (Specify type of modification and authority)

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

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

Please see the attached amendments to the RFP and responses to questions.

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

15A. NAME AND TITLE OF SIGNER (Type or print)	16A. NAME AND TITLE OF CONTRACTING OFFICER (Type or print)
Michael P. Norcio Chairman and Chief Executive Officer	Joseph Widdup
15B. CONTRACTOR/OFFEROR (Signature of person authorized to sign)	15C. DATE SIGNED June 27, 2012
16B. UNITED STATES OF AMERICA BY (Signature of Contracting Officer)	16C. DATE SIGNED

NSN 7540-01-152-8070
PREVIOUS EDITION NOT USABLE

STANDARD FORM 30 (REV. 10-83)
Prescribed by GSA - FAR (48 CFR) 53.243

AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT	BPA NO.	1. CONTRACT ID CODE	PAGE 1	OF PAGES 1

2. AMENDMENT/MODIFICATION NO.	3. EFFECTIVE DATE	4. REQUISITION/PURCHASE REQ. NO.	5. PROJECT NO. (If applicable)
A003		NRC-HQ-R-33-0067	

6. ISSUED BY CODE 3100

U.S. Nuclear Regulatory Commission
Div. of Contracts
Attn: Jordan Pulaski
Mail Stop: TWB-01-B10M
Washington, DC 20555

7. ADMINISTERED BY (If other than Item 6) CODE 3100

U.S. Nuclear Regulatory Commission
Div. of Contracts
Mail Stop: TWB-01-B10M

Washington, DC 20555

8. NAME AND ADDRESS OF CONTRACTOR (No., street, county, State and ZIP Code)

To all Offerors/Bidders
MAR, Incorporated
1803 Research Boulevard, Suite 204
Rockville, MD 20850

(X) 9A. AMENDMENT OF SOLICITATION NO.
NRC-HQ-12-R-33-0067

9B. DATED (SEE ITEM 11)
X 05-31-2012

10A. MODIFICATION OF CONTRACT/ORDER NO.

10B. DATED (SEE ITEM 13)

CODE FACILITY CODE

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

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

12. ACCOUNTING AND APPROPRIATION DATA (If required) N/A.

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

(X) A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: (Specify authority) THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NO. IN ITEM 10A.

B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES (such as changes in paying office, appropriation date, etc.) SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(b).

C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF:

D. OTHER (Specify type of modification and authority)

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

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

The due date for proposals, specified in box 8 of the RFP cover page (SF 1449), is extended to:

June 27, 2012 by 4:00 P.M.

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

15A. NAME AND TITLE OF SIGNER (Type or print)	16A. NAME AND TITLE OF CONTRACTING OFFICER (Type or print)
Michael P. Norcio Chairman and Chief Executive Officer	Joseph Widdup
15B. CONTRACTOR/OFFEROR (Signature of person authorized to sign)	15C. DATE SIGNED June 27, 2012
	16B. UNITED STATES OF AMERICA BY (Signature of Contracting Officer)
	16C. DATE SIGNED

NSN 7540-01-152-8070
PREVIOUS EDITION NOT USABLE

STANDARD FORM 30 (REV. 10-83)
Prescribed by GSA - FAR (48 CFR) 53.243

AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT

BPA NO.	1. CONTRACT ID CODE	PAGE	OF
		1	1

2. AMENDMENT/MODIFICATION NO.	3. EFFECTIVE DATE	4. REQUISITION/PURCHASE REQ. NO.	5. PROJECT NO.(If applicable)
A004		NRC-HQ-R-33-0067	

6. ISSUED BY CODE 3100

U.S. Nuclear Regulatory Commission
Div. of Contracts
Attn: Jordan Pulaski
Mail Stop: TWB-01-B10M
Washington, DC 20555

7. ADMINISTERED BY (If other than Item 6) CODE 3100

U.S. Nuclear Regulatory Commission
Div. of Contracts
Mail Stop: TWB-01-B10M

Washington, DC 20555

8. NAME AND ADDRESS OF CONTRACTOR (No., street, county, State and ZIP Code)

MAR, Incorporated
1803 Research Boulevard, Suite 204
Rockville, MD 20850

(X) 9A. AMENDMENT OF SOLICITATION NO.
NRC-HQ-12-R-33-0067

9B. DATED (SEE ITEM 11)
X 05-31-2012

10A. MODIFICATION OF CONTRACT/ORDER NO.

10B. DATED (SEE ITEM 13)

CODE FACILITY CODE

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

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

12. ACCOUNTING AND APPROPRIATION DATA (If required) N/A.

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

(X) A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: (Specify authority) THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NO. IN ITEM 10A.

B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES (such as changes in paying office, appropriation date, etc.) SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(b).

C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF:

D. OTHER (Specify type of modification and authority)

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

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

If the GSA eBuy site cannot handle the file size of an offeror's proposal, offeror's may alternatively submit their proposals directly to jordan.pulaski@nrc.gov with the subject line "NRC-HQ-12-R-33-0067 Proposal."

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

15A. NAME AND TITLE OF SIGNER (Type or print)	16A. NAME AND TITLE OF CONTRACTING OFFICER (Type or print)
Michael P. Norcio Chairman and CEO	Joseph Widdup
15B. CONTRACTOR/OFFEROR (Signature of person authorized to sign)	15C. DATE SIGNED June 27, 2012
16B. UNITED STATES OF AMERICA BY _____ (Signature of Contracting Officer)	16C. DATE SIGNED

NSN 7540-01-152-8070
PREVIOUS EDITION NOT USABLE

STANDARD FORM 30 (REV. 10-83)
Prescribed by GSA - FAR (48 CFR) 53.243

2.0 PURCHASING SYSTEM ACCEPTANCE/APPROVAL

RFP Section E.9, page 5

The following memorandum provides MAR's certification of an adequate accounting and billing system.

DEFENSE CONTRACT AUDIT AGENCY
Columbia Branch Office
One Mall North, Suite 200
10025 Governor Warfield Parkway
Columbia, MD 21044
410 964-2060 FAX: 410 997-3237

6311-431

10 July 1998

MEMORANDUM FOR DEFENSE FINANCE AND ACCOUNTING SERVICE

SUBJECT: Authorization for Direct Submission of Public Vouchers

MAR, Inc. (1) maintains an adequate billing system and (2) submits its incurred proposals in accordance with FAR 52.216-7, Allowable Cost and Payment contract clause. Therefore, in accordance with Defense Federal Acquisition Regulation Supplement (DFARS) 242.803(b0(i)(C), this contractor is permitted to directly submit public vouchers on government contracts without DCAA advance approval. By attaching one copy of this memorandum, and indicating in the signature block of the voucher that "Direct Submission [is] Authorized," the contractor is representing that DCAA has authorized direct submission of public vouchers to DFAS by MAR, Inc. DCAA will continue to review MAR, Inc.'s procedures for preparing public vouchers as part of our ongoing surveillance of the contractor's billing system. The contractor's CAGE (Commercial and Government Entity) code is 2F821.

Please direct any questions regarding this memorandum to Mr. John Pizzillo, Supervisory Auditor, at (410) 964-2060.

Mark S. Moser
Branch Manager, DCAA
Columbia Branch Office

3.0 RFP PROVISIONS E.1 AND E.4

RFP Section E.9, page 5

3.1 MAR, Incorporated's Response to RFP Provisions E.1 and E.4

3.1.1 MAR, Incorporated's Response to RFP Provision E.1 2052.209-71 Contractor Organizational Conflicts Of Interest (Representation) (Oct 1999)

I represent to the best of my knowledge and belief that:

The award to MAR, Incorporated of a contract or the modification of an existing contract does / / does not /X/ involve situations or relationships of the type set forth in 48 CFR 2009.570-3(b).

(a) If the representation, as completed, indicates that situations or relationships of the type set forth in 48 CFR 2009.570-3(b) are involved, or the contracting officer otherwise determines that potential organizational conflicts of interest exist, the Offeror shall provide a statement in writing which describes in a concise manner all relevant factors bearing on his representation to the contracting officer. If the contracting officer determines that organizational conflicts exist, the following actions may be taken:

(1) Impose appropriate conditions which avoid such conflicts,

(2) Disqualify the Offeror, or

(3) Determine that it is otherwise in the best interest of the United States to seek award of the contract under the waiver provisions of 48 CFR 2009-570-9.

(b) The refusal to provide the representation required by 48 CFR 2009.570-4(b), or upon request of the contracting officer, the facts required by 48 CFR 2009.570-3(b), must result in disqualification of the Offeror for award.

Signature

June 27, 2012
Date

Michel P. Norcio,
Chairman and Chief Executive Officer
Name and Title

3.1.2 MAR, Incorporated's Response to RFP Provision E.4 2052.209-70 Current/Former Agency Employee Involvement (Oct 1999)

(a) The following representation is required by the NRC Acquisition Regulation 2009.105-70(b). It is not NRC policy to encourage Offerors and Contractors to propose current/former agency employees to perform work under NRC contracts and as set forth in the above cited provision, the use of such employees may, under certain conditions, adversely affect NRC's consideration of non-competitive proposals and task orders.

(b) There ( ) are (**X**) are no current/former NRC employees (including special Government employees performing services as experts, advisors, consultants, or members of advisory committees) who have been or will be involved, directly or indirectly, in developing the offer, or in negotiating on behalf of the Offeror, or in managing, administering, or performing any contract, consultant agreement, or subcontract resulting from this offer. For each individual so identified, the Technical and Management proposal must contain, as a separate attachment, the name of the individual, the individual's title while employed by the NRC, the date individual left NRC, and a brief description of the individual's role under this proposal.

Signature

June 27, 2012
Date

Michel P. Norcio,
Chairman and Chief Executive Officer
Name and Title

3.2 MAR, Incorporated's Subcontractors' Response to RFP Provisions E.1 and E.4

3.2.1 CACI's Response to RFP Provisions E.1 and E.4

MEMORANDUM

To: Team Members associated with the NRC CSPSS Proposal

From: MAR, Incorporated

Date: May 4, 2012

Subject: A. Organizational Conflict of Interest – Statements and Certification

B. Former NRC Employee Statement

A. ORGANIZATIONAL CONFLICT OF INTEREST
MAR, Incorporated (MAR) is submitting a proposal to the U.S. Nuclear Regulatory Commission as a Prime Contractor under the MAR GSA Alliant Contract GS06F0641Z, in response to RFP NRC-HQ-12-R-33-0067 for Cyber Security Program Support Services (CSPSS).

As a teaming partner and potential subcontractor or consultant to MAR, Incorporated for the proposal response to the NRC, CACI, INC. - FEDERAL (name of company, consultant, teaming partner) hereby certifies that there are no relevant facts that could give rise to any Organizational Conflicts of Interest (OCOI), as defined in NRC-HQ-R-33-0067 – Attachment H. We agree to immediately disclose information concerning the actual or potential conflict relating to any work under this Solicitation and award, in accordance with FAR 9.5 and Attachment H as provided.

I represent to the best of my knowledge and belief that the award of a subcontract or consultant agreement to _____ does / / does not / X / involve situations or relationships of the type set forth in 48 CFR 2009.570-3(b).

Signature: Rachel F. Mayhew
Name (printed): Rachel F. Mayhew
Title: Contracts Administrator
Date: 5-10-2012

Further:
The subcontractor shall disclose all currently active, similar types of Contracts and Subcontracts and describe the type of work being performed. (This includes support to MAR, Incorporated as either a subcontractor or consultant). Please list below.

Consulting Agreement between MAR, Incorporated (MAR) and CACI Paradigm Solutions (CACI): From 31 January through 31 December 2012, CACI is supporting MAR as a consultant to provide expertise for Enterprise Architecture in the NRC Computer Security office.

B. 2052.209-70 CURRENT/FORMER AGENCY EMPLOYEE INVOLVEMENT (OCT 1999)

(a) The following representation is required by the NRC Acquisition Regulation 2009.105-70(b). It is not NRC policy to encourage Offerors and Contractors to propose current/former agency employees to perform work under NRC contracts and as set forth in the provision cited above, the use of such employees may, under certain conditions, adversely affect NRC's consideration of non-competitive proposals and task orders.

(b) There ( ) are (X) are no current/former NRC employees (including special Government employees performing services as experts, advisors, consultants, or members of advisory committees) who have been or will be involved, directly or indirectly, in developing the offer, or in negotiating on behalf of the Offeror, or in managing, administering, or performing any contract, consultant agreement, or subcontract resulting from this offer. For each individual so identified, the Technical and Management proposal must contain, as a separate attachment, the name of the individual, the individual's title while employed by the NRC, the date individual left NRC, and a brief description of the individual's role under this proposal.

Signature: Rachel F. Mayhew
Name (printed): Rachel F. Mayhew
Title: Contracts Administrator
Date: 5-10-2012

3.2.2 Convergent's Response to RFP Provisions E.1 and E.4

MEMORANDUM

To: Team Members associated with the NRC CSPSS Proposal
From: MAR, Incorporated
Date: May 3, 2012
Subject: A. Organizational Conflict of Interest – Statements and Certification
B. Former NRC Employee Statement

A. ORGANIZATIONAL CONFLICT OF INTEREST

MAR, Incorporated (MAR) is submitting a proposal to the U.S. Nuclear Regulatory Commission as a Prime Contractor under the MAR GSA Alliant Contract GS06F0641Z, in response to RFP NRC-HQ-12-R-33-0067 for Cyber Security Program Support Services (CSPSS).

As a teaming partner and potential subcontractor or consultant to MAR, Incorporated for the proposal response to the NRC, Convergent Solutions, Inc. hereby certifies that there are no relevant facts that could give rise to any Organizational Conflicts of Interest (OCOI), as defined in NRC-HQ-R-33-0067 – Attachment H. We agree to immediately disclose information concerning the actual or potential conflict relating to any work under this Solicitation and award, in accordance with FAR 9.5 and Attachment H as provided.

I represent to the best of my knowledge and belief that the award of a subcontract or consultant agreement to Convergent does / / does not /X/ involve situations or relationships of the type set forth in 48 CFR 2009.570-3(b).

Signature: Cynthia L. Hamilton
Name (printed): Cynthia L. Hamilton
Title: Vice President, Business Development
Date7 May 2012

Further:

The subcontractor shall disclose all currently active, similar types of Contracts and Subcontracts and describe the type of work being performed. (This includes support to MAR, Incorporated as either a subcontractor or consultant). Please list below.

B. 2052.209-70 CURRENT/FORMER AGENCY EMPLOYEE INVOLVEMENT (OCT 1999)

(a) The following representation is required by the NRC Acquisition Regulation 2009.105-70(b). It is not NRC policy to encourage Offerors and Contractors to propose current/former agency employees to perform work under NRC contracts and as set forth in the provision cited above, the use of such employees may, under certain conditions, adversely affect NRC's consideration of non-competitive proposals and task orders.

(b) There ( ) are (X) are no current/former NRC employees (including special Government employees performing services as experts, advisors, consultants, or members of advisory committees) who have been or will be involved, directly or indirectly, in developing the offer, or in negotiating on behalf of the Offeror, or in managing, administering, or performing any contract, consultant agreement, or subcontract resulting from this offer. For each individual so identified, the Technical and Management proposal must contain, as a separate attachment, the name of the individual, the individual's title while employed by the NRC, the date individual left NRC, and a brief description of the individual's role under this proposal.

Signature: Cynthia L. Hamilton
Name (printed): Cynthia L. Hamilton
Title: Vice President, Business Development
Date7 May 2012

3.2.3 DCCA's Response to RFP Provisions E.1 and E.4

MEMORANDUM

To: Team Members associated with the NRC CSPSS Proposal

From: MAR, Incorporated

Date: May 3, 2012

Subject: A. Organizational Conflict of Interest – Statements and Certification

B. Former NRC Employee Statement

A. ORGANIZATIONAL CONFLICT OF INTEREST

MAR, Incorporated (MAR) is submitting a proposal to the U.S. Nuclear Regulatory Commission as a Prime Contractor under the MAR GSA Alliant Contract GS06F0641Z, in response to RFP NRC-HQ-12-R-33-0067 for Cyber Security Program Support Services (CSPSS).

As a teaming partner and potential subcontractor or consultant to MAR, Incorporated for the proposal response to the NRC, **Data Computer Corporation of America** (DCCA) (name of company, consultant, teaming partner) hereby certifies that there are no relevant facts that could give rise to any Organizational Conflicts of Interest (OCOI), as defined in NRC-HQ-R-33-0067 – Attachment H. We agree to immediately disclose information concerning the actual or potential conflict relating to any work under this Solicitation and award, in accordance with FAR 9.5 and Attachment H as provided.

I represent to the best of my knowledge and belief that the award of a subcontract or consultant agreement to DCCA does / / does not /X/ involve situations or relationships of the type set forth in 48 CFR 2009.570-3(b).

Signature: _____
Name (printed): Jacira Johnson
Title: Sr. Contracts Manager
Date: 7 May 2012

Further:

The subcontractor shall disclose all currently active, similar types of Contracts and Subcontracts and describe the type of work being performed. (This includes support to MAR, Incorporated as either a subcontractor or consultant). Please list below.

_____

_____

B. 2052.209-70 CURRENT/FORMER AGENCY EMPLOYEE INVOLVEMENT (OCT 1999)

(a) The following representation is required by the NRC Acquisition Regulation 2009.105-70(b). It is not NRC policy to encourage Offerors and Contractors to propose current/former agency employees to perform work under NRC contracts and as set forth in the provision cited above, the use of such employees may, under certain conditions, adversely affect NRC's consideration of non-competitive proposals and task orders.

(b) There ( ) are (X) are no current/former NRC employees (including special Government employees performing services as experts, advisors, consultants, or members of advisory committees) who have been or will be involved, directly or indirectly, in developing the offer, or in negotiating on behalf of the Offeror, or in managing, administering, or performing any contract, consultant agreement, or subcontract resulting from this offer. For each individual so identified, the Technical and Management proposal must contain, as a separate attachment, the name of the individual, the individual's title while employed by the NRC, the date individual left NRC, and a brief description of the individual's role under this proposal.

Signature: _____
Name (printed): Jacira Johnson
Title: Sr. Contracts Manager
Date: 7 May 2012

3.2.4 Knowledge Consulting Group's Response to RFP Provisions E.1 and E.4

MEMORANDUM

To: Team Members associated with the NRC CSPSS Proposal

From: MAR, Incorporated

Date: May 3, 2012

Subject: A. Organizational Conflict of Interest – Statements and Certification

B. Former NRC Employee Statement

A. ORGANIZATIONAL CONFLICT OF INTEREST

MAR, Incorporated (MAR) is submitting a proposal to the U.S. Nuclear Regulatory Commission as a Prime Contractor under the MAR GSA Alliant Contract GS06F0641Z, in response to RFP NRC-HQ-12-R-33-0067 for Cyber Security Program Support Services (CSPSS).

As a teaming partner and potential subcontractor or consultant to MAR, Incorporated for the proposal response to the NRC, Knowledge Consulting Group, Inc. (name of company, consultant, teaming partner) hereby certifies that there are no relevant facts that could give rise to any Organizational Conflicts of Interest (OCOI), as defined in NRC-HQ-R-33-0067 – Attachment H. We agree to immediately disclose information concerning the actual or potential conflict relating to any work under this Solicitation and award, in accordance with FAR 9.5 and Attachment H as provided.

I represent to the best of my knowledge and belief that the award of a subcontract or consultant agreement to Knowledge Consulting Group, Inc. does not involve situations or relationships of the type set forth in 48 CFR 2009.570-3(b).

Signature: _____
Name (printed): Maryann Hirsch
Title: President
Date: May 9, 2012

Further:

The subcontractor shall disclose all currently active, similar types of Contracts and Subcontracts and describe the type of work being performed. (This includes support to MAR, Incorporated as either a subcontractor or consultant). Please list below.

KCG is currently a subcontractor to Portfolio Management Consulting LLC supporting NRC Prime Contract NRC-DR-33-10-323. KCG does not have any support to MAR at this time.

B. 2052.209-70 CURRENT/FORMER AGENCY EMPLOYEE INVOLVEMENT (OCT 1999)

(a) The following representation is required by the NRC Acquisition Regulation 2009.105-70(b). It is not NRC policy to encourage Offerors and Contractors to propose current/former agency employees to perform work under NRC contracts and as set forth in the provision cited above, the use of such employees may, under certain conditions, adversely affect NRC's consideration of non-competitive proposals and task orders.

(b) There are no current/former NRC employees (including special Government employees performing services as experts, advisors, consultants, or members of advisory committees) who have been or will be involved, directly or indirectly, in developing the offer, or in negotiating on behalf of the Offeror, or in managing, administering, or performing any contract, consultant agreement, or subcontract resulting from this offer. For each individual so identified, the Technical and Management proposal must contain, as a separate attachment, the name of the individual, the individual's title while employed by the NRC, the date individual left NRC, and a brief description of the individual's role under this proposal.

Signature: _____
Name (printed): Maryann Hirsch
Title: President
Date: May 9, 2012

3.2.5 Mainstay's Response to RFP Provisions E.1 and E.4

MEMORANDUM

To: Team Members associated with the NRC CSPSS Proposal

From: MAR, Incorporated

Date: May 4, 2012

Subject: A. Organizational Conflict of Interest – Statements and Certification

B. Former NRC Employee Statement

A. ORGANIZATIONAL CONFLICT OF INTEREST

MAR, Incorporated (MAR) is submitting a proposal to the U.S. Nuclear Regulatory Commission as a Prime Contractor under the MAR GSA Alliant Contract GS06F0641Z, in response to RFP NRC-HQ-12-R-33-0067 for Cyber Security Program Support Services (CSPSS).

As a teaming partner and potential subcontractor or consultant to MAR, Incorporated for the proposal response to the NRC, Mainstay Enterprises, Inc. (name of company, consultant, teaming partner) hereby certifies that there are no relevant facts that could give rise to any Organizational Conflicts of Interest (OCOI), as defined in NRC-HQ-R-33-0067 – Attachment H. We agree to immediately disclose information concerning the actual or potential conflict relating to any work under this Solicitation and award, in accordance with FAR 9.5 and Attachment H as provided.

I represent to the best of my knowledge and belief that the award of a subcontract or consultant agreement to _Does not_____ does / / does not / / involve situations or relationships of the type set forth in 48 CFR 2009.570-3(b).

Signature: _____
Name (printed): Gaspare Aluzzo
Title: President
Date: May 7, 2012

Further:

The subcontractor shall disclose all currently active, similar types of Contracts and Subcontracts and describe the type of work being performed. (This includes support to MAR, Incorporated as either a subcontractor or consultant). Please list below.

In support of GSAINRC GS35F0229K
Order DR-33-06-317 - Fisma Support and Incident Response Support.

B. 2052.209-70 CURRENT/FORMER AGENCY EMPLOYEE INVOLVEMENT (OCT 1999)

(a) The following representation is required by the NRC Acquisition Regulation 2009.105-70(b). It is not NRC policy to encourage Offerors and Contractors to propose current/former agency employees to perform work under NRC contracts and as set forth in the provision cited above, the use of such employees may, under certain conditions, adversely affect NRC's consideration of non-competitive proposals and task orders.

(b) There ( ) are (x) are no current/former NRC employees (including special Government employees performing services as experts, advisors, consultants, or members of advisory committees) who have been or will be involved, directly or indirectly, in developing the offer, or in negotiating on behalf of the Offeror, or in managing, administering, or performing any contract, consultant agreement, or subcontract resulting from this offer. For each individual so identified, the Technical and Management proposal must contain, as a separate attachment, the name of the individual, the individual's title while employed by the NRC, the date individual left NRC, and a brief description of the individual's role under this proposal.

Signature: _____
Name (printed): Gaspare Aluzzo
Title: President
Date: May 7, 2012

3.2.6 Prometheus Global's Response to RFP Provisions E.1 and E.4

MEMORANDUM

To: Team Members associated with the NRC CSPSS Proposal

From: MAR, Incorporated

Date: May 4, 2012

Subject: A. Organizational Conflict of Interest – Statements and Certification

B. Former NRC Employee Statement

A. ORGANIZATIONAL CONFLICT OF INTEREST

MAR, Incorporated (MAR) is submitting a proposal to the U.S. Nuclear Regulatory Commission as a Prime Contractor under the MAR GSA Alliant Contract GS06F0641Z, in response to RFP NRC-HQ-12-R-33-0067 for Cyber Security Program Support Services (CSPSS).

As a teaming partner and potential subcontractor or consultant to MAR, Incorporated for the proposal response to the NRC, Prometheus Global, Inc. (name of company, consultant, teaming partner) hereby certifies that there are no relevant facts that could give rise to any Organizational Conflicts of Interest (OCOI), as defined in NRC-HQ-R-33-0067 – Attachment H. We agree to immediately disclose information concerning the actual or potential conflict relating to any work under this Solicitation and award, in accordance with FAR 9.5 and Attachment H as provided.

I represent to the best of my knowledge and belief that the award of a subcontract or consultant agreement to Prometheus Global, Inc. does/ / does not / / involve situations or relationships of the type set forth in 48 CFR 2009.570-3(b).

Signature: _____

Name (printed): Michael T. Shinn

Title: Chief Executive Officer

Date: May 16, 2012

Further:

The subcontractor shall disclose all currently active, similar types of Contracts and Subcontracts and describe the type of work being performed. (This includes support to MAR, Incorporated as either a subcontractor or consultant). Please list below.

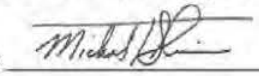
Subcontractor to MAR Incorporated for CSPSS contract and NSIR contract

Period of Performance: May 2009 - Current

B. 2052.209-70 CURRENT/FORMER AGENCY EMPLOYEE INVOLVEMENT (OCT 1999)

(a) The following representation is required by the NRC Acquisition Regulation 2009.105-70(b). It is not NRC policy to encourage Offerors and Contractors to propose current/former agency employees to perform work under NRC contracts and as set forth in the provision cited above, the use of such employees may, under certain conditions, adversely affect NRC's consideration of non-competitive proposals and task orders.

(b) There ( ) are (X) are no current/former NRC employees (including special Government employees performing services as experts, advisors, consultants, or members of advisory committees) who have been or will be involved, directly or indirectly, in developing the offer, or in negotiating on behalf of the Offeror, or in managing, administering, or performing any contract, consultant agreement, or subcontract resulting from this offer. For each individual so identified, the Technical and Management proposal must contain, as a separate attachment, the name of the individual, the individual's title while employed by the NRC, the date individual left NRC, and a brief description of the individual's role under this proposal.

Signature: 

Name (printed): Michael T. Shinn

Title: Chief Executive Officer

Date: May 16, 2012

3.2.7 Securicon's Response to RFP Provisions E.1 and E.4

MEMORANDUM

To: Team Members associated with the NRC CSPSS Proposal

From: MAR, Incorporated

Date: June 4, 2012

Subject: A. Organizational Conflict of Interest – Statements and Certification

B. Former NRC Employee Statement

A. ORGANIZATIONAL CONFLICT OF INTEREST

MAR, Incorporated (MAR) is submitting a proposal to the U.S. Nuclear Regulatory Commission as a Prime Contractor under the MAR GSA Alliant Contract GS06F0641Z, in response to RFP NRC-HQ-12-R-33-0067 for Cyber Security Program Support Services (CSPSS).

As a teaming partner and potential subcontractor or consultant to MAR, Incorporated for the proposal response to the NRC, Securicon, LLC (name of company, consultant, teaming partner) hereby certifies that there are no relevant facts that could give rise to any Organizational Conflicts of Interest (OCOI), as defined in NRC-HQ-R-33-0067 – Attachment H. We agree to immediately disclose information concerning the actual or potential conflict relating to any work under this Solicitation and award, in accordance with FAR 9.5 and Attachment H as provided.

I represent to the best of my knowledge and belief that the award of a subcontract or consultant agreement to Securicon, LLC ~~does~~ / / does not /X / involve situations or relationships of the type set forth in 48 CFR 2009.570-3(b).

Signature:
Name (printed): Paul W. Hurley
Title: CEO
Date: May 7, 2012

Further:

The subcontractor shall disclose all currently active, similar types of Contracts and Subcontracts and describe the type of work being performed. (This includes support to MAR, Incorporated as either a subcontractor or consultant). Please list below.

None.

B. 2052.209-70 CURRENT/FORMER AGENCY EMPLOYEE INVOLVEMENT (OCT 1999)

(a) The following representation is required by the NRC Acquisition Regulation 2009.105-70(b). It is not NRC policy to encourage Offerors and Contractors to propose current/former agency employees to perform work under NRC contracts and as set forth in the provision cited above, the use of such employees may, under certain conditions, adversely affect NRC's consideration of non-competitive proposals and task orders.

(b) There ( ) are (X) are no current/former NRC employees (including special Government employees performing services as experts, advisors, consultants, or members of advisory committees) who have been or will be involved, directly or indirectly, in developing the offer, or in negotiating on behalf of the Offeror, or in managing, administering, or performing any contract, consultant agreement, or subcontract resulting from this offer. For each individual so identified, the Technical and Management proposal must contain, as a separate attachment, the name of the individual, the individual's title while employed by the NRC, the date individual left NRC, and a brief description of the individual's role under this proposal.

Signature:
Name (printed): Paul W. Hurley
Title: CEO
Date: May 7, 2012

4.0 COST/PRICE

RFP Section E.9, page 5

Our proposed cost/price was developed to align with Attachment D of the RFQ. We reviewed all of the SOW referenced technical documents including applicable NRC Management Directives, CSO Guidance and Standards, Federal Information Processing Standards (FIPS), National Institutes of Standards and Technology (NIST), Office of Management and Budget (OMB), Government Accountability Office (GAO), Committee on National Security Systems (CNSS), and others. We developed a staffing resource plan and the associated levels of effort needed to complete all of the task areas outlined in the SOW. We selected 14 GSA ASB labor categories from the 80 available labor categories to fulfill the requirements. We further examined this mix of resources and associated effort to arrive at labor hour rate discounts that provide the NRC with the necessary skill sets to address the technical complexities of the task areas at an economical cost.

Table 1, MAR Proposed Labor Categories and Discounted Hourly Rates, provides our discounted GSA ASB labor hour rates for the selected GSA ASB labor categories and is organized as follows:

- **Column 1:** The GSA ASB labor categories MAR has selected to support CSPSS.
- **Column 2:** The corresponding GSA ASB Year 4 Government Site Hourly Labor Rate.
- **Column 3:** MAR's proposed discount percentage for the Year 4 Government Site Rate, N/A indicates that we are not proposing a Government Site rate for the Labor Category.
- **Column 4:** The MAR discounted proposed Government Site labor rate for CSPSS.
- **Column 5:** The corresponding GSA ASB Year 4 Contractor Site Hourly Labor Rate.
- **Column 6:** MAR's proposed discount percentage for the Year 4 Contractor Site Rate, N/A indicates that we are not proposing a Contractor Site rate for the Labor Category.
- **Column 7:** The discounted proposed Contractor Site labor rate for CSPSS.

Table 1. MAR Proposed Labor Categories and Discounted Hourly Rates

GSA ASB Year 4 (February 3, 2012 through February 2, 2013) Labor Category	Government Site			Contractor Site		
	GSA ASB GWAC Year 4 Rate	% Discount	GSA ASB GWAC Discounted Rate	GSA ASB GWAC Year 4 Rate	% Discount	GSA ASB GWAC Discounted Rate
Administration/ Clerical (Senior)	$63.85	(b)(4)		$89.52	(b)(4)	
Computer Forensic and Intrusion Analyst	$185.24			$259.71		
Financial Analyst	$81.51			$114.28		
Information Assurance/Security Specialist (Entry Level)	$68.81			$96.47		
Information Assurance/Security Specialist (Journeyman)	$89.99			$126.17		
Information Assurance/Security Specialist (Senior)	$111.15			$155.83		
Information Assurance/Security Specialist (Master)	$127.02			$178.09		
Program Manager	$142.90			$200.35		

Table 1. MAR Proposed Labor Categories and Discounted Hourly Rates

GSA ASB Year 4 (February 3, 2012 through February 2, 2013) Labor Category	Government Site			Contractor Site		
	GSA ASB GWAC Year 4 Rate	% Discount	GSA ASB GWAC Discounted Rate	GSA ASB GWAC Year 4 Rate	% Discount	GSA ASB GWAC Discounted Rate
Project Manager	$127.04	(b)(4)		$178.12	(b)(4)	
Quality Assurance Specialist (Journeyman)	$89.99			$126.17		
Subject Matter Expert (Journeyman)	$106.48			$149.29		
Subject Matter Expert (Senior)	$127.04			$178.12		
Subject Matter Expert (Master)	$158.77			$222.60		
Technical Writer	$89.99			$126.17		

Our estimates for labor and associated discounts are based on our team's experience gained at the NRC along with the historical analysis we conducted to validate our cost realism. We are providing additional discounts by proposing a minimal (b)(4) escalation for Option 3 and Option 5 hourly rates only. This represents a significant discount on the current (b)(4) annual escalation from the MAR GSA ASB rates. We are not proposing any escalation on the FFP CLINs.

Using the labor categories and rates presented in Table 1, our cost/price proposal is based on historical costs, labor resourcing, and performance metrics compiled using the TaskTracker system and other data within the MAR Project Management Oversight System (PMOS). We have an established performance record of introducing efficiencies and constantly adjusting our labor mix to provide the NRC with cost effective services often under compressed or changing schedules.

By following many of the same technical and administrative processes outlined in our technical proposal, we have maintained a positive EVM under CISSS since September 2007 as shown in Figure 7, page 16, Volume I. We are still operating within our CISSS contract ceiling as we are completing an extended sixth year of the contract. This was accomplished by the NRC reinvesting many of the contract cost savings back into the program. Through this reinvestment, MAR working with the NRC was able to establish the NRC Information System Security Program as one of only three government agencies with compliant programs in place for all eleven Cyber Security Areas as noted in the March 7, 2012, *OMB Fiscal Year 2011 Report to Congress on the Implementation of the Federal Information Security Management Act of 2002.*

Firm Fixed Price CLINS

For each of the FFP CLINS, those marked in Attachment D with a Unit of "EA", we reviewed the scope of services listed in the SOW Cross Reference column of Attachment D. We examined our historical performance metrics and lessons learned for comparable activities performed under the current NRC CISSS contract. These FFP activities included Authorizations, Laptop Authorizations, Continuous Monitoring, Vulnerability Assessments, Security Impact Assessments, and Cyber Security Role Based Awareness Training. After conducting an in-depth trend analysis on the activities and associated metrics that matched each of the Attachment D FFP activities, we determined the past 18 to 24 months provided us with a more realistic set of data to use as a basis for developing our proposed unit costs. From this data we developed a series of FFP unit prices that are based on an optimal mix of skills and hours to

efficiently provide the services and produce the associated deliverables for each activity. We believe through the execution of our technical approach presented in Volume I the NRC will continue to have an ongoing maturity of their Cyber Security Program. From this process MAR will deliver consistent and efficient authorization activities resulting in a continuation of successful cost management for all of the NRC stakeholders that we have supported over the past six years.

Time and Materials CLIN

For each of the T&M CLINS, those marked in Attachment D with a Unit of "HR", we reviewed the scope of services in the SOW Cross Reference column of Attachment D. We examined our historical performance metrics and lessons learned for comparable activities performed under the current NRC CISSS contract. From our performance metrics, along with historical performance combined with our technical approach, we established an appropriate mix of labor to accomplish the scope of work outlined in the SOW. We mapped the labor mix to the appropriate labor categories along with an associated percentage of time each of the labor categories will perform on the activity. Using the NRC provided hours along with our associated labor category percentages we computed the hours for each appropriate labor category and applied our GSA ASB discounted hourly rates to arrive at a unit price by labor category within the CLIN. The ceiling price is a total of all unit prices within each CLIN.

Attachment D

Using Attachment D from the RFQ as a model we developed tabs within the Excel spreadsheet for the base year and each option year along with a cost summary tab. The Excel spreadsheet is provided as an attachment to this proposal. We have also included the spreadsheet tables in this section. The cost/price spreadsheet is organized as follows:

- **Column 1:** "Contract Line Item Number (CLIN)" is the same as the NRC provided in Attachment D.
- **Column 2:** "SOW Cross Reference" is the same as the NRC provided in Attachment D.
- **Column 3:** "Description" was modified to add "and GSA Alliant Small Business GWAC Labor Category."
  - For each T&M CLIN ("HR") we included additional rows under the CLIN to indicate the one or more MAR proposed Labor Categories to support the CLIN.
  - For FFP CLINs ("EA") we did not make any changes.
- **Column 4:** MAR modified this column from "Unit" to "Unit Total."
  - For T&M CLINs ("HR") we included the NRC provided number of hours and an additional breakdown of MAR labor hours by their proposed Labor Categories; the MAR proposed hourly distributions total up to the NRC proposed hours for each CLIN.
  - For FFP CLINs ("EA") we did not make any changes to the NRC provided values.
- **Column 5:** "Unit Price" contains unit pricing for T&M and FFP CLINs as follows:
  - For T&M CLINs ("HR") we provided the MAR GSA ASB Discounted Hourly Labor Rate for their associated Labor Categories.
  - For FFP CLINs ("EA") we provided the unit price for each FFP unit of work as described in Column 3.
- **Column 6:** "Ceiling Price" contains the total ceiling price for each CLIN as follows:
  - For T&M CLINs (HR) we multiplied the Unit Total (column 4 number of hours) by Unit Price (column 5 discounted hourly rate) for each proposed labor category and added the total of all labor categories under each CLIN to arrive at the total CLIN ceiling price.

- For FFP CLINs ("EA") we multiplied the NRC provided Unit Total (column 4) by MAR Unit Price (column 5) for each CLIN to arrive at the ceiling price.

We made no change to the NRC supplied Other Direct Costs (ODC) at the end of the non-optional CLIN pricing. At the end of each table we provided:

- **Total without Optional CLINS:** The total of all ceiling prices for the non-optional CLINS and the NRC supplied ODC.
- **Total of Optional CLINS:** The total of all ceiling prices for the optional CLINS.
- **Grand Total for the Base or specific Option Year:** The total for all ceiling prices (optional and non-optional CLINS) and the NRC supplied ODC.

4.1 CSPSS Base Period Cost/Price

4.1.1 CSPSS Base Period Cost/Price – Part 1

Base Period: August 31, 2012 - August 30, 2013					
Contract Line Item Number (CLIN)	SOW Cross Reference	Description and GSA Alliant Small Business GWAC Labor Category	Unit Total	Unit Price	Ceiling Price
0001	**Section 8.0**	**Overall Contract Responsibilities**	**HR**		
0001A		Financials and Status Reporting	(b)(4)		$219,884.80
		Administration/Clerical (Senior)			
		Financial Analyst			
0001B		Support for Scanning Laptops and Other Tools			$109,961.20
		Information Assurance/Security Specialist (Entry Level)			
0001C		Quality Assurance for Overall contract Only			$251,426.50
		Quality Assurance Specialist (Journeyman)			
		Subject Matter Expert (Senior)			
0002	**Section 8.1.2**	**Project Plan and Project Manager Support**	**HR**		
0002A		Project Manager	(b)(4)		$391,679.20
		Project Manager			
		Project Manager			
0002B		Program Manager			$48,588.00
		Program Manager			
0003	**Section 8.2.2**	**Classified Processing Support**	**HR**		
			(b)(4)		$64,406.00
		Level)			
		Information Assurance/Security Specialist (Master)			
		Subject Matter Expert (Senior)			
0004	**Section 8.2.3**	**Evaluate New Technology**	**HR**		
			(b)(4)		$94,145.50
		Information Assurance/Security Specialist (Entry Level)			
		Subject Matter Expert (Master)			
0005	**Section 8.2.4**	**Best Practices**	**HR**		
			(b)(4)		$52,351.00
		Information Assurance/Security Specialist (Entry Level)			
		Subject Matter Expert (Master)			
		Technical Writer			
0006	**Section 8.3.1**	**Authorization**	**EA**		
0006A		Small system (Less than 15 components) -Low Sensitivity	(b)(4)		$65,738.60
0006B		Small system (Less than 15 components) - Moderate Sensitivity			$447,484.80
0006C		Medium system (16-50 components) - Moderate Sensitivity			$542,219.60
0006D		Medium system (16-50 components) - High Sensitivity			$127,829.16
0006E		Large system (51-199 or greater components) - Moderate Sensitivity			$74,621.14
0006F		Large system (51-199 or greater components) - High Sensitivity			$402,485.50

Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this proposal.

4.1.2 CSPSS Base Period Cost/Price – Part 2

Base Period: August 31, 2012 - August 30, 2013					
Contract Line Item Number (CLIN)	**SOW Cross Reference**	**Description and GSA Alliant Small Business GWAC Labor Category**	**Unit Total**	**Unit Price**	**Ceiling Price**
0007	**Section 8.3.2**	**Laptop Authorization**	**EA**		
0007A		General Use	(b)(4)		$10,809.20
0007B		SGI			$6,755.75
0007C		Classified			$2,702.30
0008	**Section 8.4**	**Continuous Monitoring Support**	**EA**		
0008A		Annual Security Controls Test	(b)(4)		$252,000.00
0008B		Continuous Monitoring Activities for a Small System (Less than 15 components) -Low Sensitivity			$90,323.01
0008C		Continuous Monitoring Activities for a Small system (Less than 15 components) - Moderate Sensitivity			$158,187.35
0008D		Continuous Monitoring Activities for a Medium system (16-50 components) - Moderate Sensitivity			$229,088.25
0008E		Continuous Monitoring Activities for a Medium system (16-50 components) - High Sensitivity			$147,607.95
0008F		Continuous Monitoring Activities for a Large system (51-199 components) - Moderate Sensitivity			$49,809.45
0008G		Continuous Monitoring Activities for a Large system (51-199 components) - High Sensitivity			$174,615.15
0009	**Section 8.4**	**Continuous Monitoring Support**	**HR**		
0009A		Security Engineering Support	(b)(4)		$276,494.40
		Information Assurance/Security Specialist (Entry Level)			
		Information Assurance/Security Specialist (Journeyman)			
		Information Assurance/Security Specialist (Senior)			
		Information Assurance/Security Specialist (Master)			
		Technical Writer			
0009B		Process Support			$186,270.40
		Information Assurance/Security Specialist (Master)			
0010	**Section 8.5**	**Data Calls**	**HR**		
			(b)(4)		$24,565.80
		Information Assurance/Security Specialist (Entry Level)			
0011	**Section 8.6.1**	**Incident Response**	**HR**		
			(b)(4)		$210,184.00
		Subject Matter Expert (Senior)			
0012	**Section 8.6.2**	**Security Architecture**	**HR**		
			(b)(4)		$150,052.60
		Computer Forensic and Intrusion Analyst			
		Subject Matter Expert (Master)			

4.1.3 CSPSS Base Period Cost/Price – Part 3

Base Period: August 31, 2012 - August 30, 2013					
Contract Line Item Number (CLIN)	SOW Cross Reference	Description and GSA Alliant Small Business GWAC Labor Category	Unit Total	Unit Price	Ceiling Price
0013	**Section 8.6.3**	**Vulnerability Assessment**	**EA**		
0013A		Small system (Less than 15 components)	(b)(4)		$18,000.00
0013B		Medium system (16-50 components)			$63,660.64
0013C		Large system (51-199 components)			$50,798.08
0014	**Section 8.6.4**	**Source Code Reviews**	**HR**		
			(b)(4)		$51,440.00
		Subject Matter Expert (Master)			
0015	**Section 8.6.5**	**Penetration Testing**	**HR**		
			(b)(4)		$78,999.20
		Information Assurance/Security Specialist (Journeyman)			
		Subject Matter Expert (Senior)			
		Subject Matter Expert (Master)			
		Technical Writer			
0016	**Section 8.6.6**	**Security Impact Assessments**	**EA**		
0016A		Small system (Less than 10 components tested)	(b)(4)		$43,500.00
0016B		Medium system (11-60 components tested)			$77,885.52
0016C		Large system (60-120 components tested)			$33,626.36
0017	**Section 8.7.1**	**Cyber Security Policy**	**HR**		
			(b)(4)		$46,917.00
		Subject Matter Expert (Journeyman)			
		Technical Writer			
0018	**Section 8.7.2**	**Processes, Procedures, Templates, Checklists, Standards, and Guidance**	**HR**		
			(b)(4)		$74,013.00
		Information Assurance/Security Specialist (Journeyman)			
		Subject Matter Expert (Master)			
		Technical Writer			
0019	**Section 8.7.7**	**Communications**	**HR**		
			(b)(4)		$58,565.40
		Information Assurance/Security Specialist (Entry Level)			
		Subject Matter Expert (Master)			
		Technical Writer			
1020	**N/A**	**Other Direct Costs (Not to Exceed)**			$160,000.00

Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this proposal.

4.1.4 CSPSS Base Period Cost/Price – Part 4

Base Period: August 31, 2012 - August 30, 2013 [OPTIONAL CLINs]					
Contract Line Item Number (CLIN)	SOW Cross Reference	Description and GSA Alliant Small Business GWAC Labor Category	Unit Total	Unit Price	Ceiling Price
0021	Section 8.2.1	**Residual Risk per system**	HR		
		Special systems (infrastructure)	(b)(4)		$76,144.40
		Information Assurance/Security Specialist (Entry Level)			
		Information Assurance/Security Specialist (Journeyman)			
		Information Assurance/Security Specialist (Master)			
		Subject Matter Expert (Master)			
		Technical Writer			
0022	Section 8.3.1	**Authorization**	HR		
		Special system (At least 200 components)	(b)(4)		$114,992.28
		Information Assurance/Security Specialist (Entry Level)			
		Information Assurance/Security Specialist (Senior)			
		Information Assurance/Security Specialist (Master)			
		Quality Assurance Specialist (Journeyman)			
		Technical Writer			
0023	Section 8.4	**Continuous Monitoring Support**	HR		
		Special system (At least 200 components)	(b)(4)		$105,940.60
		Information Assurance/Security Specialist (Entry Level)			
		Information Assurance/Security Specialist (Journeyman)			
		Information Assurance/Security Specialist (Master)			
		Quality Assurance Specialist (Journeyman)			
		Subject Matter Expert (Senior)			
		Technical Writer			
0024	Section 8.6.3	**Vulnerability Assessment**	HR		
		Special system (At least 200 components)	(b)(4)		$70,705.00
		Information Assurance/Security Specialist (Journeyman)			
		Information Assurance/Security Specialist (Senior)			
		Information Assurance/Security Specialist (Master)			
		Quality Assurance Specialist (Journeyman)			
		Technical Writer			
0025	Section 8.6.6	**Security Impact Assessments**	HR		
		Special system (121 or more components tested)	(b)(4)		$58,300.60
		Information Assurance/Security Specialist (Entry Level)			
		Information Assurance/Security Specialist (Master)			
		Quality Assurance Specialist (Journeyman)			
		Technical Writer			
0026	Section 8.7.3	**Cyber Security Relevant Business Solutions**	HR		
			(b)(4)		$82,494.00
		Information Assurance/Security Specialist (Journeyman)			
		Subject Matter Expert (Master)			
		Technical Writer			

4.1.5 CSPSS Base Period Cost/Price – Part 5

Base Period: August 31, 2012 - August 30, 2013 [OPTIONAL CLINs]					
Contract Line Item Number (CLIN)	**SOW Cross Reference**	**Description and GSA Alliant Small Business GWAC Labor Category**	**Unit Total**	**Unit Price**	**Ceiling Price**
0027	**Section 8.7.4**	**Cyber Security Awareness Training**	**HR**		
			(b)(4)		$26,516.40
		Information Assurance/Security Specialist (Entry Level)			
		Information Assurance/Security Specialist (Master)			
		Subject Matter Expert (Master)			
		Technical Writer			
0028	**Section 8.7.5**	**Cyber Security Role Based Awareness Training (development and instruction)**	**EA**		
		Course Development per day	(b)(4)		$63,987.04
0029	**Section 8.7.5**	**Cyber Security Role Based Awareness Training (development and instruction)**	**HR**		
		Instruction per day (42 days)	(b)(4)		$32,724.12
		Information Assurance/Security Specialist (Entry Level)			
		Information Assurance/Security Specialist (Master)			
		Subject Matter Expert (Senior)			
		Subject Matter Expert (Master)			
0030	**Section 8.7.6**	**Cyber Security Conference**	**HR**		
			(b)(4)		$51,308.50
		Information Assurance/Security Specialist (Journeyman)			
		Information Assurance/Security Specialist (Master)			
		Subject Matter Expert (Master)			
				Total Without Optional CLINs	**$5,619,691.81**
				Total of Optional CLINs	**$683,112.94**
				Base Year Grand Total	**$6,302,804.75**

4.2 CSPSS Option 1 Cost/Price

4.2.1 CSPSS Option 1 Cost/Price – Part 1

Option 1: August 31, 2013 - August 30, 2014					
Contract Line Item Number (CLIN)	SOW Cross Reference	Description and GSA Alliant Small Business GWAC Labor Category	Unit Total	Unit Price	Ceiling Price
0001	**Section 8.0**	**Overall Contract Responsibilities**	**HR**		
0001A		Financials and Status Reporting	(b)(4)		$219,884.80
		Administration/Clerical (Senior)			
		Financial Analyst			
0001B		Support for Scanning Laptops and Other Tools			$109,961.20
		Information Assurance/Security Specialist (Entry Level)			
0001C		Quality Assurance for Overall contract Only			$251,426.50
		Quality Assurance Specialist (Journeyman)			
		Subject Matter Expert (Senior)			
0002	**Section 8.1.2**	**Project Plan and Project Manager Support**	**HR**		
0002A		Project Manager	(b)(4)		$391,679.20
		Project Manager			
		Project Manager			
0002B		Program Manager			$48,588.00
		Program Manager			
0003	**Section 8.2.2**	**Classified Processing Support**	**HR**		
			(b)(4)		$64,406.00
		Information Assurance/Security Specialist (Entry Level)			
		Information Assurance/Security Specialist (Master)			
		Subject Matter Expert (Senior)			
0004	**Section 8.2.3**	**Evaluate New Technology**	**HR**		
			(b)(4)		$94,145.50
		Information Assurance/Security Specialist (Entry Level)			
		Subject Matter Expert (Master)			
0005	**Section 8.2.4**	**Best Practices**	**HR**		
			(b)(4)		$52,351.00
		Information Assurance/Security Specialist (Entry Level)			
		Subject Matter Expert (Master)			
		Technical Writer			
0006	**Section 8.3.1**	**Authorization**	**EA**		
0006A		Small system (Less than 15 components) -Low Sensitivity	(b)(4)		$65,738.60
0006B		Small system (Less than 15 components) - Moderate Sensitivity			$447,484.80
0006C		Medium system (16-50 components) - Moderate Sensitivit			$542,219.60
0006D		Medium system (16-50 components) - High Sensitivity			$127,829.16
0006E		Large system (51-199 or greater components) - Moderate Sensitivity			$74,621.14
0006F		Large system (51-199 or greater components) - High Sensitivity			$402,485.50

4.2.2 CSPSS Option 1 Cost/Price – Part 2

Option 1: August 31, 2013 - August 30, 2014					
Contract Line Item Number (CLIN)	**SOW Cross Reference**	**Description and GSA Alliant Small Business GWAC Labor Category**	**Unit Total**	**Unit Price**	**Ceiling Price**
0007	**Section 8.3.2**	**Laptop Authorization**	**EA**		
0007A		General Use	(b)(4)		$10,809.20
0007B		SGI			$6,755.75
0007C		Classified			$2,702.30
0008	**Section 8.4**	**Continuous Monitoring Support**	**EA**		
0008A		Annual Security Controls Test	(b)(4)		$252,000.00
0008B		Continuous Monitoring Activities for a Small System (Less than 15 components) -Low Sensitivity			$90,323.01
0008C		Continuous Monitoring Activities for a Small system (Less than 15 components) - Moderate Sensitivity			$158,187.35
0008D		Continuous Monitoring Activities for a Medium system (16-50 components) - Moderate Sensitivity			$229,088.25
0008E		Continuous Monitoring Activities for a Medium system (16-50 components) - High Sensitivity			$147,607.95
0008F		Continuous Monitoring Activities for a Large system (51-199 components) - Moderate Sensitivity			$49,809.45
0008G		Continuous Monitoring Activities for a Large system (51-199 components) - High Sensitivity			$174,615.15
0009	**Section 8.4**	**Continuous Monitoring Support**	**HR**		
0009A		Security Engineering Support	(b)(4)		$276,494.40
		Information Assurance/Security Specialist (Entry Level)			
		Information Assurance/Security Specialist (Journeyman			
		Information Assurance/Security Specialist (Senior)			
		Information Assurance/Security Specialist (Master)			
		Technical Writer			
0009B		Process Support			$186,270.40
		Information Assurance/Security Specialist (Master)			
0010	**Section 8.5**	**Data Calls**	**HR**		
			(b)(4)		$24,565.80
		Information Assurance/Security Specialist (Entry Level)			
0011	**Section 8.6.1**	**Incident Response**	**HR**		
			(b)(4)		$210,184.00
		Subject Matter Expert (Senior)			
0012	**Section 8.6.2**	**Security Architecture**	**HR**		
			(b)(4)		$150,052.60
		Computer Forensic and Intrusion Analyst			
		Subject Matter Expert (Master)			

4.2.3 CSPSS Option 1 Cost/Price – Part 3

Option 1: August 31, 2013 - August 30, 2014					
Contract Line Item Number (CLIN)	SOW Cross Reference	Description and GSA Alliant Small Business GWAC Labor Category	Unit Total	Unit Price	Ceiling Price
0013	**Section 8.6.3**	**Vulnerability Assessment**	**EA**		
0013A		Small system (Less than 15 components)	(b)(4)		$18,000.00
0013B		Medium system (16-50 components)			$63,660.64
0013C		Large system (51-199 components)			$50,798.08
0014	**Section 8.6.4**	**Source Code Reviews**	**HR**		
			(b)(4)		$51,440.00
		Subject Matter Expert (Master)			
0015	**Section 8.6.5**	**Penetration Testing**	**HR**		
			(b)(4)		$78,999.20
		Information Assurance/Security Specialist (Journeyman)			
		Subject Matter Expert (Senior)			
		Subject Matter Expert (Master)			
		Technical Writer			
0016	**Section 8.6.6**	**Security Impact Assessments**	**EA**		
0016A		Small system (Less than 10 components tested)	(b)(4)		$43,500.00
0016B		Medium system (11-60 components tested)			$77,885.52
0016C		Large system (60-120 components tested)			$33,626.36
0017	**Section 8.7.1**	**Cyber Security Policy**	**HR**		
			(b)(4)		$46,917.00
		Subject Matter Expert (Journeyman)			
		Technical Writer			
0018	**Section 8.7.2**	**Processes, Procedures, Templates, Checklists, Standards, and Guidance**	**HR**		
			(b)(4)		$74,013.00
		Information Assurance/Security Specialist (Journeyman)			
		Subject Matter Expert (Master)			
		Technical Writer			
0019	**Section 8.7.7**	**Communications**	**HR**		
			(b)(4)		$58,565.40
		Information Assurance/Security Specialist (Entry Level)			
		Subject Matter Expert (Master)			
		Technical Writer			
1020	**N/A**	**Other Direct Costs (Not to Exceed)**	N/A	N/A	$160,000.00

Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this proposal.

4.2.4 CSPSS Option 1 Cost/Price – Part 4

Option 1: August 31, 2013 - August 30, 2014 [OPTIONAL CLINs]					
Contract Line Item Number (CLIN)	SOW Cross Reference	Description and GSA Alliant Small Business GWAC Labor Category	Unit Total	Unit Price	Ceiling Price
0021	Section 8.2.1	**Residual Risk per system**	HR		
		Special systems (infrastructure)	(b)(4)		$76,144.40
		Information Assurance/Security Specialist (Entry Level)			
		Information Assurance/Security Specialist (Journeyman)			
		Information Assurance/Security Specialist (Master)			
		Subject Matter Expert (Master)			
		Technical Writer			
0022	Section 8.3.1	**Authorization**	HR		
		Special system (At least 200 components)	(b)(4)		$114,992.28
		Information Assurance/Security Specialist (Entry Level)			
		Information Assurance/Security Specialist (Senior)			
		Information Assurance/Security Specialist (Master)			
		Quality Assurance Specialist (Journeyman)			
		Technical Writer			
0023	Section 8.4	**Continuous Monitoring Support**	HR		
		Special system (At least 200 components)	(b)(4)		$105,940.60
		Information Assurance/Security Specialist (Entry Level)			
		Information Assurance/Security Specialist (Journeyman)			
		Information Assurance/Security Specialist (Master)			
		Quality Assurance Specialist (Journeyman)			
		Subject Matter Expert (Senior)			
		Technical Writer			
0024	Section 8.6.3	**Vulnerability Assessment**	HR		
		Special system (At least 200 components)	(b)(4)		$70,705.00
		Information Assurance/Security Specialist (Journeyman)			
		Information Assurance/Security Specialist (Senior)			
		Information Assurance/Security Specialist (Master)			
		Quality Assurance Specialist (Journeyman)			
		Technical Writer			
0025	Section 8.6.6	**Security Impact Assessments**	HR		
		Special system (121 or more components tested)	(b)(4)		$58,300.60
		Information Assurance/Security Specialist (Entry Level)			
		Information Assurance/Security Specialist (Master)			
		Quality Assurance Specialist (Journeyman)			
		Technical Writer			
0026	Section 8.7.3	**Cyber Security Relevant Business Solutions**	HR		
			(b)(4)		$82,494.00
		Information Assurance/Security Specialist (Journeyman)			
		Subject Matter Expert (Master)			
		Technical Writer			

4.2.5 CSPSS Option 1 Cost/Price – Part 5

Option 1: August 31, 2013 - August 30, 2014 [OPTIONAL CLINs]					
Contract Line Item Number (CLIN)	**SOW Cross Reference**	**Description and GSA Alliant Small Business GWAC Labor Category**	**Unit Total**	**Unit Price**	**Ceiling Price**
0027	**Section 8.7.4**	**Cyber Security Awareness Training**	**HR**		
			(b)(4)		$26,516.40
		Information Assurance/Security Specialist (Entry Level)			
		Information Assurance/Security Specialist (Master)			
		Subject Matter Expert (Master)			
		Technical Writer			
0028	**Section 8.7.5**	**Cyber Security Role Based Awareness Training (development and instruction)**	**EA**		
		Course Development per day	(b)(4)		$63,987.04
0029	**Section 8.7.5**	**Cyber Security Role Based Awareness Training (development and instruction)**	**HR**		
		Instruction per day (42 days)	(b)(4)		$32,724.12
		Information Assurance/Security Specialist (Entry Level)			
		Information Assurance/Security Specialist (Master)			
		Subject Matter Expert (Senior)			
		Subject Matter Expert (Master)			
0030	**Section 8.7.6**	**Cyber Security Conference**	**HR**		
			(b)(4)		$51,308.50
		Information Assurance/Security Specialist (Journeyman			
		Information Assurance/Security Specialist (Master)			
		Subject Matter Expert (Master)			
				Total Without Optional CLINs	**$5,619,691.81**
				Total of Optional CLINs	**$683,112.94**
				Option 1 Grand Total	**$6,302,804.75**

4.3 CSPSS Option 2 Cost/Price

4.3.1 CSPSS Option 2 Cost/Price – Part 1

Option 2: August 31, 2014 - August 30, 2015					
Contract Line Item Number (CLIN)	SOW Cross Reference	Description and GSA Alliant Small Business GWAC Labor Category	Unit Total	Unit Price	Ceiling Price
0001	**Section 8.0**	**Overall Contract Responsibilities**	**HR**		
0001A		Financials and Status Reporting	(b)(4)		$219,884.80
		Administration/Clerical (Senior)			
		Financial Analyst			
0001B		Support for Scanning Laptops and Other Tools			$109,961.20
		Information Assurance/Security Specialist (Entry Level)			
0001C		Quality Assurance for Overall contract Only			$251,426.50
		Quality Assurance Specialist (Journeyman)			
		Subject Matter Expert (Senior)			
0002	**Section 8.1.2**	**Project Plan and Project Manager Support**	**HR**		
0002A		Project Manager	(b)(4)		$391,679.20
		Project Manager			
		Project Manager			
0002B		Program Manager			$48,588.00
		Program Manager			
0003	**Section 8.2.2**	**Classified Processing Support**	**HR**		
			(b)(4)		$64,406.00
		Information Assurance/Security Specialist (Entry Level)			
		Information Assurance/Security Specialist (Master)			
		Subject Matter Expert (Senior)			
0004	**Section 8.2.3**	**Evaluate New Technology**	**HR**		
			(b)(4)		$94,145.50
		Information Assurance/Security Specialist (Entry Level)			
		Subject Matter Expert (Master)			
0005	**Section 8.2.4**	**Best Practices**	**HR**		
			(b)(4)		$52,351.00
		Information Assurance/Security Specialist (Entry Level)			
		Subject Matter Expert (Master)			
		Technical Writer			
0006	**Section 8.3.1**	**Authorization**	**EA**		
0006A		Small system (Less than 15 components) -Low Sensitivity	(b)(4)		$65,738.60
0006B		Small system (Less than 15 components) - Moderate Sensitivity			$447,484.80
0006C		Medium system (16-50 components) - Moderate Sensitivity			$542,219.60
0006D		Medium system (16-50 components) - High Sensitivity			$127,829.16
0006E		Large system (51-199 or greater components) - Moderate Sensitivity			$74,621.14
0006F		Large system (51-199 or greater components) - High Sensitivity			$402,485.50

4.3.2 CSPSS Option 2 Cost/Price – Part 2

Option 2: August 31, 2014 - August 30, 2015					
Contract Line Item Number (CLIN)	**SOW Cross Reference**	**Description and GSA Alliant Small Business GWAC Labor Category**	**Unit Total**	**Unit Price**	**Ceiling Price**
0007	**Section 8.3.2**	**Laptop Authorization**	**EA**		
0007A		General Use	(b)(4)		$10,809.20
0007B		SGI			$6,755.75
0007C		Classified			$2,702.30
0008	**Section 8.4**	**Continuous Monitoring Support**	**EA**		
0008A		Annual Security Controls Test	(b)(4)		$252,000.00
0008B		Continuous Monitoring Activities for a Small System (Less than 15 components) -Low Sensitivity			$90,323.01
0008C		Continuous Monitoring Activities for a Small system (Less than 15 components) - Moderate Sensitivity			$158,187.35
0008D		Continuous Monitoring Activities for a Medium system (16-50 components) - Moderate Sensitivity			$229,088.25
0008E		Continuous Monitoring Activities for a Medium system (16-50 components) - High Sensitivity			$147,607.95
0008F		Continuous Monitoring Activities for a Large system (51-199 components) - Moderate Sensitivity			$49,809.45
0008G		Continuous Monitoring Activities for a Large system (51-199 components) - High Sensitivity			$174,615.15
0009	**Section 8.4**	**Continuous Monitoring Support**	**HR**		
0009A		Security Engineering Support	(b)(4)		$276,494.40
		Information Assurance/Security Specialist (Entry Level)			
		Information Assurance/Security Specialist (Journeyman)			
		Information Assurance/Security Specialist (Senior)			
		Information Assurance/Security Specialist (Master)			
		Technical Writer			
0009B		Process Support			$186,270.40
		Information Assurance/Security Specialist (Master)			
0010	**Section 8.5**	**Data Calls**	**HR**		
			(b)(4)		$24,565.80
		Information Assurance/Security Specialist (Entry Level)			
0011	**Section 8.6.1**	**Incident Response**	**HR**		
			(b)(4)		$210,184.00
		Subject Matter Expert (Senior)			
0012	**Section 8.6.2**	**Security Architecture**	**HR**		
			(b)(4)		$150,052.60
		Computer Forensic and Intrusion Analyst			
		Subject Matter Expert (Master)			

4.3.3 CSPSS Option 2 Cost/Price – Part 3

Option 2: August 31, 2014 - August 30, 2015					
Contract Line Item Number (CLIN)	SOW Cross Reference	Description and GSA Alliant Small Business GWAC Labor Category	Unit Total	Unit Price	Ceiling Price
0013	**Section 8.6.3**	**Vulnerability Assessment**	**EA**		
0013A		Small system (Less than 15 components)	(b)(4)		$18,000.00
0013B		Medium system (16-50 components)			$63,660.64
0013C		Large system (51-199 components)			$50,798.08
0014	**Section 8.6.4**	**Source Code Reviews**	**HR**		
			(b)(4)		$51,440.00
		Subject Matter Expert (Master)			
0015	**Section 8.6.5**	**Penetration Testing**	**HR**		
			(b)(4)		$78,999.20
		Information Assurance/Security Specialist (Journeyman)			
		Subject Matter Expert (Senior)			
		Subject Matter Expert (Master)			
		Technical Writer			
0016	**Section 8.6.6**	**Security Impact Assessments**	**EA**		
0016A		Small system (Less than 10 components tested)	(b)(4)		$43,500.00
0016B		Medium system (11-60 components tested)			$77,885.52
0016C		Large system (60-120 components tested)			$33,626.36
0017	**Section 8.7.1**	**Cyber Security Policy**	**HR**		
			(b)(4)		$46,917.00
		Subject Matter Expert (Journeyman)			
		Technical Writer			
0018	**Section 8.7.2**	**Processes, Procedures, Templates, Checklists, Standards, and Guidance**	**HR**		
			(b)(4)		$74,013.00
		Information Assurance/Security Specialist (Journeyman)			
		Subject Matter Expert (Master)			
		Technical Writer			
0019	**Section 8.7.7**	**Communications**	**HR**		
			(b)(4)		$58,565.40
		Information Assurance/Security Specialist (Entry Level)			
		Subject Matter Expert (Master)			
		Technical Writer			
1020	**N/A**	**Other Direct Costs (Not to Exceed)**	N/A	N/A	$160,000.00

4.3.4 CSPSS Option 2 Cost/Price – Part 4

Option 2: August 31, 2014 - August 30, 2015 [OPTIONAL CLINs]					
Contract Line Item Number (CLIN)	SOW Cross Reference	Description and GSA Alliant Small Business GWAC Labor Category	Unit Total	Unit Price	Ceiling Price
0021	Section 8.2.1	**Residual Risk per system**	HR		
		Special systems (infrastructure)	(b)(4)		$76,144.40
		Information Assurance/Security Specialist (Entry Level)			
		Information Assurance/Security Specialist (Journeyman)			
		Information Assurance/Security Specialist (Master)			
		Subject Matter Expert (Master)			
		Technical Writer			
0022	Section 8.3.1	**Authorization**	HR		
		Special system (At least 200 components)	(b)(4)		$114,992.28
		Information Assurance/Security Specialist (Entry Level)			
		Information Assurance/Security Specialist (Senior)			
		Information Assurance/Security Specialist (Master)			
		Quality Assurance Specialist (Journeyman)			
		Technical Writer			
0023	Section 8.4	**Continuous Monitoring Support**	HR		
		Special system (At least 200 components)	(b)(4)		$105,940.60
		Information Assurance/Security Specialist (Entry Level)			
		Information Assurance/Security Specialist (Journeyman)			
		Information Assurance/Security Specialist (Master)			
		Quality Assurance Specialist (Journeyman)			
		Subject Matter Expert (Senior)			
		Technical Writer			
0024	Section 8.6.3	**Vulnerability Assessment**	HR		
		Special system (At least 200 components)	(b)(4)		$70,705.00
		Information Assurance/Security Specialist (Journeyman)			
		Information Assurance/Security Specialist (Senior)			
		Information Assurance/Security Specialist (Master)			
		Quality Assurance Specialist (Journeyman)			
		Technical Writer			
0025	Section 8.6.6	**Security Impact Assessments**	HR		
		Special system (121 or more components tested)	(b)(4)		$58,300.60
		Information Assurance/Security Specialist (Entry Level)			
		Information Assurance/Security Specialist (Master)			
		Quality Assurance Specialist (Journeyman)			
		Technical Writer			
0026	Section 8.7.3	**Cyber Security Relevant Business Solutions**	HR		
			(b)(4)		$82,494.00
		Information Assurance/Security Specialist (Journeyman)			
		Subject Matter Expert (Master)			
		Technical Writer			

4.3.5 CSPSS Option 2 Cost/Price – Part 5

Option 2: August 31, 2014 - August 30, 2015 [OPTIONAL CLINs]					
Contract Line Item Number (CLIN)	**SOW Cross Reference**	**Description and GSA Alliant Small Business GWAC Labor Category**	**Unit Total**	**Unit Price**	**Ceiling Price**
0027	**Section 8.7.4**	**Cyber Security Awareness Training**	**HR**		
			(b)(4)		$26,516.40
		Information Assurance/Security Specialist (Entry Level)			
		Information Assurance/Security Specialist (Master)			
		Subject Matter Expert (Master)			
		Technical Writer			
0028	**Section 8.7.5**	**Cyber Security Role Based Awareness Training (development and instruction)**	**EA**		
		Course Development per day	(b)(4)		$63,987.04
0029	**Section 8.7.5**	**Cyber Security Role Based Awareness Training (development and instruction)**	**HR**		
		Instruction per day (42 days)	(b)(4)		$32,724.12
		Information Assurance/Security Specialist (Entry Level)			
		Information Assurance/Security Specialist (Master)			
		Subject Matter Expert (Senior)			
		Subject Matter Expert (Master)			
0030	**Section 8.7.6**	**Cyber Security Conference**	**HR**		
			(b)(4)		$51,308.50
		Information Assurance/Security Specialist (Journeyman)			
		Information Assurance/Security Specialist (Master)			
		Subject Matter Expert (Master)			
				Total Without Optional CLINs	**$5,619,691.81**
				Total of Optional CLINs	**$683,112.94**
				Option 2 Grand Total	**$6,302,804.75**

4.4 CSPSS Option 3 Cost/Price

4.4.1 CSPSS Option 3 Cost/Price – Part 1

Option 3: August 31, 2015 - August 30, 2016					
Contract Line Item Number (CLIN)	SOW Cross Reference	Description and GSA Alliant Small Business GWAC Labor Category	Unit Total	Unit Price	Ceiling Price
0001	**Section 8.0**	**Overall Contract Responsibilities**	**HR**		
0001A		Financials and Status Reporting	(b)(4)		$222,084.40
		Administration/Clerical (Senior)			
		Financial Analyst			
0001B		Support for Scanning Laptops and Other Tools			$111,051.60
		Information Assurance/Security Specialist (Entry Level)			
0001C		Quality Assurance for Overall contract Only			$253,936.30
		Quality Assurance Specialist (Journeyman)			
		Subject Matter Expert (Senior)			
0002	**Section 8.1.2**	**Project Plan and Project Manager Support**	**HR**		
0002A		Project Manager	(b)(4)		$395,589.60
		Project Manager			
		Project Manager			
0002B		Program Manager			$49,072.00
		Program Manager			
0003	**Section 8.2.2**	**Classified Processing Support**	**HR**		
			(b)(4)		$65,048.75
		Information Assurance/Security Specialist (Entry Level)			
		Information Assurance/Security Specialist (Master)			
		Subject Matter Expert (Senior)			
0004	**Section 8.2.3**	**Evaluate New Technology**	**HR**		
			(b)(4)		$95,083.50
		Information Assurance/Security Specialist (Entry Level)			
		Subject Matter Expert (Master)			
0005	**Section 8.2.4**	**Best Practices**	**HR**		
			(b)(4)		$52,874.50
		Information Assurance/Security Specialist (Entry Level)			
		Subject Matter Expert (Master)			
		Technical Writer			
0006	**Section 8.3.1**	**Authorization**	**EA**		
0006A		Small system (Less than 15 components) -Low Sensitivity	(b)(4)		$65,738.60
0006B		Small system (Less than 15 components) - Moderate Sensitivity			$447,484.80
0006C		Medium system (16-50 components) - Moderate Sensitivity			$542,219.60
0006D		Medium system (16-50 components) - High Sensitivity			$127,829.16
0006E		Large system (51-199 or greater components) - Moderate Sensitivity			$74,621.14
0006F		Large system (51-199 or greater components) - High Sensitivity			$402,485.50

4.4.2 CSPSS Option 3 Cost/Price – Part 2

Option 3: August 31, 2015 - August 30, 2016					
Contract Line Item Number (CLIN)	**SOW Cross Reference**	**Description and GSA Alliant Small Business GWAC Labor Category**	**Unit Total**	**Unit Price**	**Ceiling Price**
0007	**Section 8.3.2**	**Laptop Authorization**	**EA**		
0007A		General Use	(b)(4)		$10,809.20
0007B		SGI			$6,755.75
0007C		Classified			$2,702.30
0008	**Section 8.4**	**Continuous Monitoring Support**	**EA**		
0008A		Annual Security Controls Test	(b)(4)		$252,000.00
0008B		Continuous Monitoring Activities for a Small System (Less than 15 components) -Low Sensitivity			$90,323.01
0008C		Continuous Monitoring Activities for a Small system (Less than 15 components) - Moderate Sensitivity			$158,187.35
0008D		Continuous Monitoring Activities for a Medium system (16-50 components) - Moderate Sensitivity			$229,088.25
0008E		Continuous Monitoring Activities for a Medium system (16-50 components) - High Sensitivity			$147,607.95
0008F		Continuous Monitoring Activities for a Large system (51-199 components) - Moderate Sensitivity			$49,809.45
0008G		Continuous Monitoring Activities for a Large system (51-199 components) - High Sensitivity			$174,615.15
0009	**Section 8.4**	**Continuous Monitoring Support**	**HR**		
0009A		Security Engineering Support	(b)(4)		$279,250.08
		Information Assurance/Security Specialist (Entry Level)			
		Information Assurance/Security Specialist (Journeyman)			
		Information Assurance/Security Specialist (Senior)			
		Information Assurance/Security Specialist (Master)			
		Technical Writer			
0009B		Process Support			$188,131.60
		Information Assurance/Security Specialist (Master)			
0010	**Section 8.5**	**Data Calls**	**HR**		
			(b)(4)		$24,809.40
		Information Assurance/Security Specialist (Entry Level)			
0011	**Section 8.6.1**	**Incident Response**	**HR**		
			(b)(4)		$212,289.60
		Subject Matter Expert (Senior)			
0012	**Section 8.6.2**	**Security Architecture**	**HR**		
			(b)(4)		$151,556.20
		Computer Forensic and Intrusion Analyst			
		Subject Matter Expert (Master)			

4.4.3 CSPSS Option 3 Cost/Price – Part 3

Option 3: August 31, 2015 - August 30, 2016					
Contract Line Item Number (CLIN)	SOW Cross Reference	Description and GSA Alliant Small Business GWAC Labor Category	Unit Total	Unit Price	Ceiling Price
0013	**Section 8.6.3**	**Vulnerability Assessment**	**EA**		
0013A		Small system (Less than 15 components)	(b)(4)		$18,000.00
0013B		Medium system (16-50 components)			$63,660.64
0013C		Large system (51-199 components)			$50,798.08
0014	**Section 8.6.4**	**Source Code Reviews**	**HR**		
			(b)(4)		$51,956.00
		Subject Matter Expert (Master)			
0015	**Section 8.6.5**	**Penetration Testing**	**HR**		
			(b)(4)		$79,788.50
		Information Assurance/Security Specialist (Journeyman)			
		Subject Matter Expert (Senior)			
		Subject Matter Expert (Master)			
		Technical Writer			
0016	**Section 8.6.6**	**Security Impact Assessments**	**EA**		
0016A		Small system (Less than 10 components tested)	(b)(4)		$43,500.00
0016B		Medium system (11-60 components tested)			$77,885.52
0016C		Large system (60-120 components tested)			$33,626.36
0017	**Section 8.7.1**	**Cyber Security Policy**	**HR**		
			(b)(4)		$47,388.00
		Subject Matter Expert (Journeyman)			
		Technical Writer			
0018	**Section 8.7.2**	**Processes, Procedures, Templates, Checklists, Standards, and Guidance**	**HR**		
			(b)(4)		$74,753.50
		Information Assurance/Security Specialist (Journeyman)			
		Subject Matter Expert (Master)			
		Technical Writer			
0019	**Section 8.7.7**	**Communications**	**HR**		
			(b)(4)		$59,151.80
		Information Assurance/Security Specialist (Entry Level)			
		Subject Matter Expert (Master)			
		Technical Writer			
1020	**N/A**	**Other Direct Costs (Not to Exceed)**	N/A	N/A	$160,000.00

4.4.4 CSPSS Option 3 Cost/Price – Part 4

Option 3: August 31, 2015 - August 30, 2016 [OPTIONAL CLINs]					
Contract Line Item Number (CLIN)	SOW Cross Reference	Description and GSA Alliant Small Business GWAC Labor Category	Unit Total	Unit Price	Ceiling Price
0021	Section 8.2.1	**Residual Risk per system**	HR		
		Special systems (infrastructure)	(b)(4)		$76,903.60
		Information Assurance/Security Specialist (Entry Level)			
		Information Assurance/Security Specialist (Journeyman)			
		Information Assurance/Security Specialist (Master)			
		Subject Matter Expert (Master)			
		Technical Writer			
0022	Section 8.3.1	**Authorization**	HR		
		Special system (At least 200 components)	(b)(4)		$116,138.04
		Information Assurance/Security Specialist (Entry Level)			
		Information Assurance/Security Specialist (Senior)			
		Information Assurance/Security Specialist (Master)			
		Quality Assurance Specialist (Journeyman)			
		Technical Writer			
0023	Section 8.4	**Continuous Monitoring Support**	HR		
		Special system (At least 200 components)	(b)(4)		$106,994.96
		Information Assurance/Security Specialist (Entry Level)			
		Information Assurance/Security Specialist (Journeyman)			
		Information Assurance/Security Specialist (Master)			
		Quality Assurance Specialist (Journeyman)			
		Subject Matter Expert (Senior)			
		Technical Writer			
0024	Section 8.6.3	**Vulnerability Assessment**	HR		
		Special system (At least 200 components)	(b)(4)		$71,409.32
		Information Assurance/Security Specialist (Journeyman)			
		Information Assurance/Security Specialist (Senior)			
		Information Assurance/Security Specialist (Master)			
		Quality Assurance Specialist (Journeyman)			
		Technical Writer			
0025	Section 8.6.6	**Security Impact Assessments**	HR		
		Special system (121 or more components tested)	(b)(4)		$58,881.80
		Information Assurance/Security Specialist (Entry Level)			
		Information Assurance/Security Specialist (Master)			
		Quality Assurance Specialist (Journeyman)			
		Technical Writer			
0026	Section 8.7.3	**Cyber Security Relevant Business Solutions**	HR		
			(b)(4)		$83,318.00
		Information Assurance/Security Specialist (Journeyman)			
		Subject Matter Expert (Master)			
		Technical Writer			

4.4.5 CSPSS Option 3 Cost/Price – Part 5

Option 3: August 31, 2015 - August 30, 2016 [OPTIONAL CLINs]					
Contract Line Item Number (CLIN)	SOW Cross Reference	Description and GSA Alliant Small Business GWAC Labor Category	Unit Total	Unit Price	Ceiling Price
0027	Section 8.7.4	**Cyber Security Awareness Training**	HR		
			(b)(4)		$26,781.60
		Information Assurance/Security Specialist (Entry Level)			
		Information Assurance/Security Specialist (Master)			
		Subject Matter Expert (Master)			
		Technical Writer			
0028	Section 8.7.5	**Cyber Security Role Based Awareness Training (development and instruction)**	EA		
		Course Development per day	(b)(4)		$63,987.04
0029	Section 8.7.5	**Cyber Security Role Based Awareness Training (development and instruction)**	HR		
		Instruction per day (42 days)	(b)(4)		$33,051.32
		Information Assurance/Security Specialist (Entry Level)			
		Information Assurance/Security Specialist (Master)			
		Subject Matter Expert (Senior)			
		Subject Matter Expert (Master)			
0030	Section 8.7.6	**Cyber Security Conference**	HR		
			(b)(4)		$51,821.40
		Information Assurance/Security Specialist (Journeyman)			
		Information Assurance/Security Specialist (Master)			
		Subject Matter Expert (Master)			
				Total Without Optional CLINs	**$5,643,563.14**
				Total of Optional CLINs	**$689,287.08**
				Option 3 Grand Total	**$6,332,850.22**

4.5 CSPSS Option 4 Cost/Price

4.5.1 CSPSS Option 4 Cost/Price – Part 1

Option 4: August 31, 2016 - August 30, 2017					
Contract Line Item Number (CLIN)	SOW Cross Reference	Description and GSA Alliant Small Business GWAC Labor Category	Unit Total	Unit Price	Ceiling Price
0001	**Section 8.0**	**Overall Contract Responsibilities**	**HR**		
0001A		Financials and Status Reporting	(b)(4)		$222,084.40
		Administration/Clerical (Senior)			
		Financial Analyst			
0001B		Support for Scanning Laptops and Other Tools			$111,051.60
		Information Assurance/Security Specialist (Entry Level)			
0001C		Quality Assurance for Overall contract Only			$253,936.30
		Quality Assurance Specialist (Journeyman)			
		Subject Matter Expert (Senior)			
0002	**Section 8.1.2**	**Project Plan and Project Manager Support**	**HR**		
0002A		Project Manager	(b)(4)		$395,589.60
		Project Manager			
		Project Manager			
0002B		Program Manager			$49,072.00
		Program Manager			
0003	**Section 8.2.2**	**Classified Processing Support**	**HR**		
			(b)(4)		$65,048.75
		Information Assurance/Security Specialist (Entry Level)			
		Information Assurance/Security Specialist (Master)			
		Subject Matter Expert (Senior)			
0004	**Section 8.2.3**	**Evaluate New Technology**	**HR**		
			(b)(4)		$95,083.50
		Information Assurance/Security Specialist (Entry Level)			
		Subject Matter Expert (Master)			
0005	**Section 8.2.4**	**Best Practices**	**HR**		
			(b)(4)		$52,874.50
		Information Assurance/Security Specialist (Entry Level)			
		Subject Matter Expert (Master)			
		Technical Writer			
0006	**Section 8.3.1**	**Authorization**	**EA**		
0006A		Small system (Less than 15 components) -Low Sensitivity	(b)(4)		$65,738.60
0006B		Small system (Less than 15 components) - Moderate Sensitivity			$447,484.80
0006C		Medium system (16-50 components) - Moderate Sensitivit			$542,219.60
0006D		Medium system (16-50 components) - High Sensitivity			$127,829.16
0006E		Large system (51-199 or greater components) - Moderate Sensitivity			$74,621.14
0006F		Large system (51-199 or greater components) - High Sensitivity			$402,485.50

4.5.2 CSPSS Option 4 Cost/Price – Part 2

Option 4: August 31, 2016 - August 30, 2017					
Contract Line Item Number (CLIN)	**SOW Cross Reference**	**Description and GSA Alliant Small Business GWAC Labor Category**	**Unit Total**	**Unit Price**	**Ceiling Price**
0007	**Section 8.3.2**	**Laptop Authorization**	**EA**		
0007A		General Use	(b)(4)		$10,809.20
0007B		SGI			$6,755.75
0007C		Classified			$2,702.30
0008	**Section 8.4**	**Continuous Monitoring Support**	**EA**		
0008A		Annual Security Controls Test	(b)(4)		$252,000.00
0008B		Continuous Monitoring Activities for a Small System (Less than 15 components) -Low Sensitivity			$90,323.01
0008C		Continuous Monitoring Activities for a Small system (Less than 15 components) - Moderate Sensitivity			$158,187.35
0008D		Continuous Monitoring Activities for a Medium system (16-50 components) - Moderate Sensitivity			$229,088.25
0008E		Continuous Monitoring Activities for a Medium system (16-50 components) - High Sensitivity			$147,607.95
0008F		Continuous Monitoring Activities for a Large system (51-199 components) - Moderate Sensitivity			$49,809.45
0008G		Continuous Monitoring Activities for a Large system (51-199 components) - High Sensitivity			$174,615.15
0009	**Section 8.4**	**Continuous Monitoring Support**	**HR**		
0009A		Security Engineering Support	(b)(4)		$279,250.08
		Information Assurance/Security Specialist (Entry Level)			
		Information Assurance/Security Specialist (Journeyman)			
		Information Assurance/Security Specialist (Senior)			
		Information Assurance/Security Specialist (Master)			
		Technical Writer			
0009B		Process Support			$188,131.60
		Information Assurance/Security Specialist (Master)			
0010	**Section 8.5**	**Data Calls**	**HR**		
			(b)(4)		$24,809.40
		Information Assurance/Security Specialist (Entry Level)			
0011	**Section 8.6.1**	**Incident Response**	**HR**		
			(b)(4)		$212,289.60
		Subject Matter Expert (Senior)			
0012	**Section 8.6.2**	**Security Architecture**	**HR**		
			(b)(4)		$151,556.20
		Computer Forensic and Intrusion Analyst			
		Subject Matter Expert (Master)			

4.5.3 CSPSS Option 4 Cost/Price – Part 3

Option 4: August 31, 2016 - August 30, 2017					
Contract Line Item Number (CLIN)	SOW Cross Reference	Description and GSA Alliant Small Business GWAC Labor Category	Unit Total	Unit Price	Ceiling Price
0013	**Section 8.6.3**	**Vulnerability Assessment**	**EA**		
0013A		Small system (Less than 15 components)	(b)(4)		$18,000.00
0013B		Medium system (16-50 components)			$63,660.64
0013C		Large system (51-199 components)			$50,798.08
0014	**Section 8.6.4**	**Source Code Reviews**	**HR**		
			(b)(4)		$51,956.00
		Subject Matter Expert (Master)			
0015	**Section 8.6.5**	**Penetration Testing**	**HR**		
			(b)(4)		$79,788.50
		Information Assurance/Security Specialist (Journeyman)			
		Subject Matter Expert (Senior)			
		Subject Matter Expert (Master)			
		Technical Writer			
0016	**Section 8.6.6**	**Security Impact Assessments**	**EA**		
0016A		Small system (Less than 10 components tested)	(b)(4)		$43,500.00
0016B		Medium system (11-60 components tested)			$77,885.52
0016C		Large system (60-120 components tested)			$33,626.36
0017	**Section 8.7.1**	**Cyber Security Policy**	**HR**		
			(b)(4)		$47,388.00
		Subject Matter Expert (Journeyman)			
		Technical Writer			
0018	**Section 8.7.2**	**Processes, Procedures, Templates, Checklists, Standards, and Guidance**	**HR**		
			(b)(4)		$74,753.50
		Information Assurance/Security Specialist (Journeyman)			
		Subject Matter Expert (Master)			
		Technical Writer			
0019	**Section 8.7.7**	**Communications**	**HR**		
			(b)(4)		$59,151.80
		Information Assurance/Security Specialist (Entry Level)			
		Subject Matter Expert (Master)			
		Technical Writer			
1020	**N/A**	**Other Direct Costs (Not to Exceed)**	N/A	N/A	$160,000.00

Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this proposal.

4.5.4 CSPSS Option 4 Cost/Price – Part 4

Option 4: August 31, 2016 - August 30, 2017 [OPTIONAL CLINs]					
Contract Line Item Number (CLIN)	SOW Cross Reference	Description and GSA Alliant Small Business GWAC Labor Category	Unit Total	Unit Price	Ceiling Price
0021	Section 8.2.1	**Residual Risk per system**	HR		
		Special systems (infrastructure)	(b)(4)		$76,903.60
		Information Assurance/Security Specialist (Entry Level)			
		Information Assurance/Security Specialist (Journeyman)			
		Information Assurance/Security Specialist (Master)			
		Subject Matter Expert (Master)			
		Technical Writer			
0022	Section 8.3.1	**Authorization**	HR		
		Special system (At least 200 components)	(b)(4)		$116,138.04
		Information Assurance/Security Specialist (Entry Level)			
		Information Assurance/Security Specialist (Senior)			
		Information Assurance/Security Specialist (Master)			
		Quality Assurance Specialist (Journeyman)			
		Technical Writer			
0023	Section 8.4	**Continuous Monitoring Support**	HR		
		Special system (At least 200 components)	(b)(4)		$106,994.96
		Information Assurance/Security Specialist (Entry Level)			
		Information Assurance/Security Specialist (Journeyman)			
		Information Assurance/Security Specialist (Master)			
		Quality Assurance Specialist (Journeyman)			
		Subject Matter Expert (Senior)			
		Technical Writer			
0024	Section 8.6.3	**Vulnerability Assessment**	HR		
		Special system (At least 200 components)	(b)(4)		$71,409.32
		Information Assurance/Security Specialist (Journeyman			
		Information Assurance/Security Specialist (Senior)			
		Information Assurance/Security Specialist (Master)			
		Quality Assurance Specialist (Journeyman)			
		Technical Writer			
0025	Section 8.6.6	**Security Impact Assessments**	HR		
		Special system (121 or more components tested)	(b)(4)		$58,881.80
		Information Assurance/Security Specialist (Entry Level)			
		Information Assurance/Security Specialist (Master)			
		Quality Assurance Specialist (Journeyman)			
		Technical Writer			
0026	Section 8.7.3	**Cyber Security Relevant Business Solutions**	HR		
			(b)(4)		$83,318.00
		Information Assurance/Security Specialist (Journeyman			
		Subject Matter Expert (Master)			
		Technical Writer			

4.5.5 CSPSS Option 4 Cost/Price – Part 5

Option 4: August 31, 2016 - August 30, 2017 [OPTIONAL CLINs]					
Contract Line Item Number (CLIN)	SOW Cross Reference	Description and GSA Alliant Small Business GWAC Labor Category	Unit Total	Unit Price	Ceiling Price
0027	Section 8.7.4	**Cyber Security Awareness Training**	HR		
			(b)(4)		$26,781.60
		Information Assurance/Security Specialist (Entry Level)			
		Information Assurance/Security Specialist (Master)			
		Subject Matter Expert (Master)			
		Technical Writer			
0028	Section 8.7.5	**Cyber Security Role Based Awareness Training (development and instruction)**	EA		
		Course Development per day	(b)(4)		$63,987.04
0029	Section 8.7.5	**Cyber Security Role Based Awareness Training (development and instruction)**	HR		
		Instruction per day (42 days)	(b)(4)		$33,051.32
		Information Assurance/Security Specialist (Entry Level)			
		Information Assurance/Security Specialist (Master)			
		Subject Matter Expert (Senior)			
		Subject Matter Expert (Master)			
0030	Section 8.7.6	**Cyber Security Conference**	HR		
			(b)(4)		$51,821.40
		Information Assurance/Security Specialist (Journeyman			
		Information Assurance/Security Specialist (Master)			
		Subject Matter Expert (Master)			
				Total Without Optional CLINs	**$5,643,563.14**
				Total of Optional CLINs	**$689,287.08**
				Option 4 Grand Total	**$6,332,850.22**

4.6 CSPSS Option 5 Cost/Price

4.6.1 CSPSS Option 5 Cost/Price – Part 1

Option 5: August 31, 2017 - August 30, 2018					
Contract Line Item Number (CLIN)	SOW Cross Reference	Description and GSA Alliant Small Business GWAC Labor Category	Unit Total	Unit Price	Ceiling Price
0001	**Section 8.0**	**Overall Contract Responsibilities**	**HR**		
0001A		Financials and Status Reporting	(b)(4)		$224,302.80
		Administration/Clerical (Senior)			
		Financial Analyst			
0001B		Support for Scanning Laptops and Other Tools			$112,160.80
		Information Assurance/Security Specialist (Entry Level)			
0001C		Quality Assurance for Overall contract Only			$256,479.00
		Quality Assurance Specialist (Journeyman)			
		Subject Matter Expert (Senior)			
0002	**Section 8.1.2**	**Project Plan and Project Manager Support**	**HR**		
0002A		Project Manager	(b)(4)		$399,537.60
		Project Manager			
		Project Manager			
0002B		Program Manager			$49,564.00
		Program Manager			
0003	**Section 8.2.2**	**Classified Processing Support**	**HR**		
			(b)(4)		$65,699.00
		Information Assurance/Security Specialist (Entry Level)			
		Information Assurance/Security Specialist (Master)			
		Subject Matter Expert (Senior)			
0004	**Section 8.2.3**	**Evaluate New Technology**	**HR**		
			(b)(4)		$96,034.00
		Information Assurance/Security Specialist (Entry Level)			
		Subject Matter Expert (Master)			
0005	**Section 8.2.4**	**Best Practices**	**HR**		
			(b)(4)		$53,403.00
		Information Assurance/Security Specialist (Entry Level)			
		Subject Matter Expert (Master)			
		Technical Writer			
0006	**Section 8.3.1**	**Authorization**	**EA**		
0006A		Small system (Less than 15 components) -Low Sensitivity	(b)(4)		$65,738.60
0006B		Small system (Less than 15 components) - Moderate Sensitivity			$447,484.80
0006C		Medium system (16-50 components) - Moderate Sensitivity			$542,219.60
0006D		Medium system (16-50 components) - High Sensitivity			$127,829.16
0006E		Large system (51-199 or greater components) - Moderate Sensitivity			$74,621.14
0006F		Large system (51-199 or greater components) - High Sensitivity			$402,485.50

4.6.2 CSPSS Option 5 Cost/Price – Part 2

Option 5: August 31, 2017 - August 30, 2018					
Contract Line Item Number (CLIN)	**SOW Cross Reference**	**Description and GSA Alliant Small Business GWAC Labor Category**	**Unit Total**	**Unit Price**	**Ceiling Price**
0007	**Section 8.3.2**	**Laptop Authorization**	**EA**		
0007A		General Use	(b)(4)		$10,809.20
0007B		SGI			$6,755.75
0007C		Classified			$2,702.30
0008	**Section 8.4**	**Continuous Monitoring Support**	**EA**		
0008A		Annual Security Controls Test	(b)(4)		$252,000.00
0008B		Continuous Monitoring Activities for a Small System (Less than 15 components) -Low Sensitivity			$90,323.01
0008C		Continuous Monitoring Activities for a Small system (Less than 15 components) - Moderate Sensitivity			$158,187.35
0008D		Continuous Monitoring Activities for a Medium system (16-50 components) - Moderate Sensitivity			$229,088.25
0008E		Continuous Monitoring Activities for a Medium system (16-50 components) - High Sensitivity			$147,607.95
0008F		Continuous Monitoring Activities for a Large system (51-199 components) - Moderate Sensitivity			$49,809.45
0008G		Continuous Monitoring Activities for a Large system (51-199 components) - High Sensitivity			$174,615.15
0009	**Section 8.4**	**Continuous Monitoring Support**	**HR**		
0009A		Security Engineering Support	(b)(4)		$282,034.56
		Information Assurance/Security Specialist (Entry Level)			
		Information Assurance/Security Specialist (Journeyman)			
		Information Assurance/Security Specialist (Senior)			
		Information Assurance/Security Specialist (Master)			
		Technical Writer			
0009B		Process Support			$190,011.60
		Information Assurance/Security Specialist (Master)			
0010	**Section 8.5**	**Data Calls**	**HR**		
			(b)(4)		$25,057.20
		Information Assurance/Security Specialist (Entry Level)			
0011	**Section 8.6.1**	**Incident Response**	**HR**		
			(b)(4)		$214,414.00
		Subject Matter Expert (Senior)			
0012	**Section 8.6.2**	**Security Architecture**	**HR**		
			(b)(4)		$153,070.20
		Computer Forensic and Intrusion Analyst			
		Subject Matter Expert (Master)			

4.6.3 CSPSS Option 5 Cost/Price – Part 3

Option 5: August 31, 2017 - August 30, 2018					
Contract Line Item Number (CLIN)	SOW Cross Reference	Description and GSA Alliant Small Business GWAC Labor Category	Unit Total	Unit Price	Ceiling Price
0013	**Section 8.6.3**	**Vulnerability Assessment**	**EA**		
0013A		Small system (Less than 15 components)	(b)(4)		$18,000.00
0013B		Medium system (16-50 components)			$63,660.64
0013C		Large system (51-199 components)			$50,798.08
0014	**Section 8.6.4**	**Source Code Reviews**	**HR**		
			(b)(4)		$52,476.00
		Subject Matter Expert (Master)			
0015	**Section 8.6.5**	**Penetration Testing**	**HR**		
			(b)(4)		$80,585.60
		Information Assurance/Security Specialist (Journeyman)			
		Subject Matter Expert (Senior)			
		Subject Matter Expert (Master)			
		Technical Writer			
0016	**Section 8.6.6**	**Security Impact Assessments**	**EA**		
0016A		Small system (Less than 10 components tested)	(b)(4)		$43,500.00
0016B		Medium system (11-60 components tested)			$77,885.52
0016C		Large system (60-120 components tested)			$33,626.36
0017	**Section 8.7.1**	**Cyber Security Policy**	**HR**		
			(b)(4)		$47,862.00
		Subject Matter Expert (Journeyman)			
		Technical Writer			
0018	**Section 8.7.2**	**Processes, Procedures, Templates, Checklists, Standards, and Guidance**	**HR**		
			(b)(4)		$75,500.50
		Information Assurance/Security Specialist (Journeyman)			
		Subject Matter Expert (Master)			
		Technical Writer			
0019	**Section 8.7.7**	**Communications**	**HR**		
			(b)(4)		$59,743.20
		Information Assurance/Security Specialist (Entry Level)			
		Subject Matter Expert (Master)			
		Technical Writer			
1020	**N/A**	**Other Direct Costs (Not to Exceed)**	N/A	N/A	$160,000.00

Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this proposal.

4.6.4 CSPSS Option 5 Cost/Price – Part 4

Option 5: August 31, 2017 - August 30, 2018 [OPTIONAL CLINs]					
Contract Line Item Number (CLIN)	SOW Cross Reference	Description and GSA Alliant Small Business GWAC Labor Category	Unit Total	Unit Price	Ceiling Price
0021	Section 8.2.1	**Residual Risk per system**	HR		
		Special systems (infrastructure)	(b)(4)		$77,671.40
		Information Assurance/Security Specialist (Entry Level)			
		Information Assurance/Security Specialist (Journeyman)			
		Information Assurance/Security Specialist (Master)			
		Subject Matter Expert (Master)			
		Technical Writer			
0022	Section 8.3.1	**Authorization**	HR		
		Special system (At least 200 components)	(b)(4)		$117,296.84
		Information Assurance/Security Specialist (Entry Level)			
		Information Assurance/Security Specialist (Senior)			
		Information Assurance/Security Specialist (Master)			
		Quality Assurance Specialist (Journeyman)			
		Technical Writer			
0023	Section 8.4	**Continuous Monitoring Support**	HR		
		Special system (At least 200 components)	(b)(4)		$108,062.52
		Information Assurance/Security Specialist (Entry Level)			
		Information Assurance/Security Specialist (Journeyman)			
		Information Assurance/Security Specialist (Master)			
		Quality Assurance Specialist (Journeyman)			
		Subject Matter Expert (Senior)			
		Technical Writer			
0024	Section 8.6.3	**Vulnerability Assessment**	HR		
		Special system (At least 200 components)	(b)(4)		$72,122.64
		Information Assurance/Security Specialist (Journeyman)			
		Information Assurance/Security Specialist (Senior)			
		Information Assurance/Security Specialist (Master)			
		Quality Assurance Specialist (Journeyman)			
		Technical Writer			
0025	Section 8.6.6	**Security Impact Assessments**	HR		
		Special system (121 or more components tested)	(b)(4)		$59,471.60
		Information Assurance/Security Specialist (Entry Level)			
		Information Assurance/Security Specialist (Master)			
		Quality Assurance Specialist (Journeyman)			
		Technical Writer			
0026	Section 8.7.3	**Cyber Security Relevant Business Solutions**	HR		
			(b)(4)		$84,150.00
		Information Assurance/Security Specialist (Journeyman)			
		Subject Matter Expert (Master)			
		Technical Writer			

4.6.5 CSPSS Option 5 Cost/Price – Part 5

Option 5: August 31, 2017 - August 30, 2018 [OPTIONAL CLINs]					
Contract Line Item Number (CLIN)	**SOW Cross Reference**	**Description and GSA Alliant Small Business GWAC Labor Category**	**Unit Total**	**Unit Price**	**Ceiling Price**
0027	**Section 8.7.4**	**Cyber Security Awareness Training**	**HR**		
			(b)(4)		$27,049.20
		Information Assurance/Security Specialist (Entry Level)			
		Information Assurance/Security Specialist (Master)			
		Subject Matter Expert (Master)			
		Technical Writer			
0028	**Section 8.7.5**	**Cyber Security Role Based Awareness Training (development and instruction)**	**EA**		
		Course Development per day	(b)(4)		$63,987.04
0029	**Section 8.7.5**	**Cyber Security Role Based Awareness Training (development and instruction)**	**HR**		
		Instruction per day (42 days)	(b)(4)		$33,381.88
		Information Assurance/Security Specialist (Entry Level)			
		Information Assurance/Security Specialist (Master)			
		Subject Matter Expert (Senior)			
		Subject Matter Expert (Master)			
0030	**Section 8.7.6**	**Cyber Security Conference**	**HR**		
			(b)(4)		$52,339.30
		Information Assurance/Security Specialist (Journeyman)			
		Information Assurance/Security Specialist (Master)			
		Subject Matter Expert (Master)			
				Total Without Optional CLINs	**$5,667,682.87**
				Total of Optional CLINs	**$695,532.42**
				Option 5 Grand Total	**$6,363,215.29**

4.7 CSPSS Option 6 Cost/Price

4.7.1 CSPSS Option 6 Cost/Price – Part 1

Option 6: August 31, 2018 - August 30, 2019					
Contract Line Item Number (CLIN)	SOW Cross Reference	Description and GSA Alliant Small Business GWAC Labor Category	Unit Total	Unit Price	Ceiling Price
0001	**Section 8.0**	**Overall Contract Responsibilities**	**HR**		
0001A		Financials and Status Reporting	(b)(4)		$224,302.80
		Administration/Clerical (Senior)			
		Financial Analyst			
0001B		Support for Scanning Laptops and Other Tools			$112,160.80
		Information Assurance/Security Specialist (Entry Level)			
0001C		Quality Assurance for Overall contract Only			$256,479.00
		Quality Assurance Specialist (Journeyman)			
		Subject Matter Expert (Senior)			
0002	**Section 8.1.2**	**Project Plan and Project Manager Support**	**HR**		
0002A		Project Manager	(b)(4)		$399,537.60
		Project Manager			
		Project Manager			
0002B		Program Manager			$49,564.00
		Program Manager			
0003	**Section 8.2.2**	**Classified Processing Support**	**HR**		
			(b)(4)		$65,699.00
		Information Assurance/Security Specialist (Entry Level)			
		Information Assurance/Security Specialist (Master)			
		Subject Matter Expert (Senior)			
0004	**Section 8.2.3**	**Evaluate New Technology**	**HR**		
			(b)(4)		$96,034.00
		Information Assurance/Security Specialist (Entry Level)			
		Subject Matter Expert (Master)			
0005	**Section 8.2.4**	**Best Practices**	**HR**		
			(b)(4)		$53,403.00
		Information Assurance/Security Specialist (Entry Level)			
		Subject Matter Expert (Master)			
		Technical Writer			
0006	**Section 8.3.1**	**Authorization**	**EA**		
0006A		Small system (Less than 15 components) -Low Sensitivity	(b)(4)		$65,738.60
0006B		Small system (Less than 15 components) - Moderate Sensitivity			$447,484.80
0006C		Medium system (16-50 components) - Moderate Sensitivity			$542,219.60
0006D		Medium system (16-50 components) - High Sensitivity			$127,829.16
0006E		Large system (51-199 or greater components) - Moderate Sensitivity			$74,621.14
0006F		Large system (51-199 or greater components) - High Sensitivity			$402,485.50

4.7.2 CSPSS Option 6 Cost/Price – Part 2

Option 6: August 31, 2018 - August 30, 2019					
Contract Line Item Number (CLIN)	**SOW Cross Reference**	**Description and GSA Alliant Small Business GWAC Labor Category**	**Unit Total**	**Unit Price**	**Ceiling Price**
0007	**Section 8.3.2**	**Laptop Authorization**	**EA**		
0007A		General Use	(b)(4)		$10,809.20
0007B		SGI			$6,755.75
0007C		Classified			$2,702.30
0008	**Section 8.4**	**Continuous Monitoring Support**	**EA**		
0008A		Annual Security Controls Test	(b)(4)		$252,000.00
0008B		Continuous Monitoring Activities for a Small System (Less than 15 components) -Low Sensitivity			$90,323.01
0008C		Continuous Monitoring Activities for a Small system (Less than 15 components) - Moderate Sensitivity			$158,187.35
0008D		Continuous Monitoring Activities for a Medium system (16-50 components) - Moderate Sensitivity			$229,088.25
0008E		Continuous Monitoring Activities for a Medium system (16-50 components) - High Sensitivity			$147,607.95
0008F		Continuous Monitoring Activities for a Large system (51-199 components) - Moderate Sensitivity			$49,809.45
0008G		Continuous Monitoring Activities for a Large system (51-199 components) - High Sensitivity			$174,615.15
0009	**Section 8.4**	**Continuous Monitoring Support**	**HR**		
0009A		Security Engineering Support	(b)(4)		$282,034.56
		Information Assurance/Security Specialist (Entry Level)			
		Information Assurance/Security Specialist (Journeyman)			
		Information Assurance/Security Specialist (Senior)			
		Information Assurance/Security Specialist (Master)			
		Technical Writer			
0009B		Process Support			$190,011.60
		Information Assurance/Security Specialist (Master)			
0010	**Section 8.5**	**Data Calls**	**HR**		
			(b)(4)		$25,057.20
		Information Assurance/Security Specialist (Entry Level)			
0011	**Section 8.6.1**	**Incident Response**	**HR**		
			(b)(4)		$214,414.00
		Subject Matter Expert (Senior)			
0012	**Section 8.6.2**	**Security Architecture**	**HR**		
			(b)(4)		$153,070.20
		Computer Forensic and Intrusion Analyst			
		Subject Matter Expert (Master)			

Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this proposal.

4.7.3 CSPSS Option 6 Cost/Price – Part 3

Option 6: August 31, 2018 - August 30, 2019					
Contract Line Item Number (CLIN)	SOW Cross Reference	Description and GSA Alliant Small Business GWAC Labor Category	Unit Total	Unit Price	Ceiling Price
0013	**Section 8.6.3**	**Vulnerability Assessment**	**EA**		
0013A		Small system (Less than 15 components)	(b)(4)		$18,000.00
0013B		Medium system (16-50 components)			$63,660.64
0013C		Large system (51-199 components)			$50,798.08
0014	**Section 8.6.4**	**Source Code Reviews**	**HR**		
			(b)(4)		$52,476.00
		Subject Matter Expert (Master)			
0015	**Section 8.6.5**	**Penetration Testing**	**HR**		
			(b)(4)		$80,585.60
		Information Assurance/Security Specialist (Journeyman)			
		Subject Matter Expert (Senior)			
		Subject Matter Expert (Master)			
		Technical Writer			
0016	**Section 8.6.6**	**Security Impact Assessments**	**EA**		
0016A		Small system (Less than 10 components tested)	(b)(4)		$43,500.00
0016B		Medium system (11-60 components tested)			$77,885.52
0016C		Large system (60-120 components tested)			$33,626.36
0017	**Section 8.7.1**	**Cyber Security Policy**	**HR**		
			(b)(4)		$47,862.00
		Subject Matter Expert (Journeyman)			
		Technical Writer			
0018	**Section 8.7.2**	**Processes, Procedures, Templates, Checklists, Standards, and Guidance**	**HR**		
			(b)(4)		$75,500.50
		Information Assurance/Security Specialist (Journeyman)			
		Subject Matter Expert (Master)			
		Technical Writer			
0019	**Section 8.7.7**	**Communications**	**HR**		
			(b)(4)		$59,743.20
		Information Assurance/Security Specialist (Entry Level)			
		Subject Matter Expert (Master)			
		Technical Writer			
1020	**N/A**	**Other Direct Costs (Not to Exceed)**	N/A	N/A	$160,000.00

4.7.4 CSPSS Option 6 Cost/Price – Part 4

Option 6: August 31, 2018 - August 30, 2019 [OPTIONAL CLINs]					
Contract Line Item Number (CLIN)	SOW Cross Reference	Description and GSA Alliant Small Business GWAC Labor Category	Unit Total	Unit Price	Ceiling Price
0021	Section 8.2.1	**Residual Risk per system**	HR		
		Special systems (infrastructure)	(b)(4)		$77,671.40
		Information Assurance/Security Specialist (Entry Level)			
		Information Assurance/Security Specialist (Journeyman)			
		Information Assurance/Security Specialist (Master)			
		Subject Matter Expert (Master)			
		Technical Writer			
0022	Section 8.3.1	**Authorization**	HR		
		Special system (At least 200 components)	(b)(4)		$117,296.84
		Information Assurance/Security Specialist (Entry Level)			
		Information Assurance/Security Specialist (Senior)			
		Information Assurance/Security Specialist (Master)			
		Quality Assurance Specialist (Journeyman)			
		Technical Writer			
0023	Section 8.4	**Continuous Monitoring Support**	HR		
		Special system (At least 200 components)	(b)(4)		$108,062.52
		Information Assurance/Security Specialist (Entry Level)			
		Information Assurance/Security Specialist (Journeyman)			
		Information Assurance/Security Specialist (Master)			
		Quality Assurance Specialist (Journeyman)			
		Subject Matter Expert (Senior)			
		Technical Writer			
0024	Section 8.6.3	**Vulnerability Assessment**	HR		
		Special system (At least 200 components)	(b)(4)		$72,122.64
		Information Assurance/Security Specialist (Journeyman			
		Information Assurance/Security Specialist (Senior)			
		Information Assurance/Security Specialist (Master)			
		Quality Assurance Specialist (Journeyman)			
		Technical Writer			
0025	Section 8.6.6	**Security Impact Assessments**	HR		
		Special system (121 or more components tested)	(b)(4)		$59,471.60
		Information Assurance/Security Specialist (Entry Level)			
		Information Assurance/Security Specialist (Master)			
		Quality Assurance Specialist (Journeyman)			
		Technical Writer			
0026	Section 8.7.3	**Cyber Security Relevant Business Solutions**	HR		
			(b)(4)		$84,150.00
		Information Assurance/Security Specialist (Journeyman)			
		Subject Matter Expert (Master)			
		Technical Writer			

4.7.5 CSPSS Option 6 Cost/Price – Part 5

Option 6: August 31, 2018 - August 30, 2019 [OPTIONAL CLINs]					
Contract Line Item Number (CLIN)	SOW Cross Reference	Description and GSA Alliant Small Business GWAC Labor Category	Unit Total	Unit Price	Ceiling Price
0027	Section 8.7.4	Cyber Security Awareness Training	HR		
			(b)(4)		$27,049.20
		Information Assurance/Security Specialist (Entry Level)			
		Information Assurance/Security Specialist (Master)			
		Subject Matter Expert (Master)			
		Technical Writer			
0028	Section 8.7.5	Cyber Security Role Based Awareness Training (development and instruction)	EA		
		Course Development per day	(b)(4)		$63,987.04
0029	Section 8.7.5	Cyber Security Role Based Awareness Training (development and instruction)	HR		
		Instruction per day (42 days)	(b)(4)		$33,381.88
		Information Assurance/Security Specialist (Entry Level)			
		Information Assurance/Security Specialist (Master)			
		Subject Matter Expert (Senior)			
		Subject Matter Expert (Master)			
0030	Section 8.7.6	Cyber Security Conference	HR		
			(b)(4)		$52,339.30
		Information Assurance/Security Specialist (Journeyman)			
		Information Assurance/Security Specialist (Master)			
		Subject Matter Expert (Master)			
				Total Without Optional CLINs	$5,667,682.87
				Total of Optional CLINs	$695,532.42
				Option 6 Grand Total	$6,363,215.29

4.8 CSPSS Option 7 Cost/Price

4.8.1 CSPSS Option 7 Cost/Price – Part 1

Option 7: August 31, 2019 - August 30, 2020					
Contract Line Item Number (CLIN)	**SOW Cross Reference**	**Description and GSA Alliant Small Business GWAC Labor Category**	**Unit Total**	**Unit Price**	**Ceiling Price**
0001	**Section 8.0**	**Overall Contract Responsibilities**	**HR**		
0001A		Financials and Status Reporting	(b)(4)		$224,302.80
		Administration/Clerical (Senior)			
		Financial Analyst			
0001B		Support for Scanning Laptops and Other Tools			$112,160.80
		Information Assurance/Security Specialist (Entry Level)			
0001C		Quality Assurance for Overall contract Only			$256,479.00
		Quality Assurance Specialist (Journeyman)			
		Subject Matter Expert (Senior)			
0002	**Section 8.1.2**	**Project Plan and Project Manager Support**	**HR**		
0002A		Project Manager	(b)(4)		$399,537.60
		Project Manager			
		Project Manager			
0002B		Program Manager			$49,564.00
		Program Manager			
0003	**Section 8.2.2**	**Classified Processing Support**	**HR**		
			(b)(4)		$65,699.00
		Information Assurance/Security Specialist (Entry Level)			
		Information Assurance/Security Specialist (Master)			
		Subject Matter Expert (Senior)			
0004	**Section 8.2.3**	**Evaluate New Technology**	**HR**		
			(b)(4)		$96,034.00
		Information Assurance/Security Specialist (Entry Level)			
		Subject Matter Expert (Master)			
0005	**Section 8.2.4**	**Best Practices**	**HR**		
			(b)(4)		$53,403.00
		Information Assurance/Security Specialist (Entry Level)			
		Subject Matter Expert (Master)			
		Technical Writer			
0006	**Section 8.3.1**	**Authorization**	**EA**		
0006A		Small system (Less than 15 components) -Low Sensitivity	(b)(4)		$65,738.60
0006B		Small system (Less than 15 components) - Moderate Sensitivity			$447,484.80
0006C		Medium system (16-50 components) - Moderate Sensitivity			$542,219.60
0006D		Medium system (16-50 components) - High Sensitivity			$127,829.16
0006E		Large system (51-199 or greater components) - Moderate Sensitivity			$74,621.14
0006F		Large system (51-199 or greater components) - High Sensitivity			$402,485.50

4.8.2 CSPSS Option 7 Cost/Price – Part 2

Option 7: August 31, 2019 - August 30, 2020					
Contract Line Item Number (CLIN)	**SOW Cross Reference**	**Description and GSA Alliant Small Business GWAC Labor Category**	**Unit Total**	**Unit Price**	**Ceiling Price**
0007	**Section 8.3.2**	**Laptop Authorization**	**EA**		
0007A		General Use	(b)(4)		$10,809.20
0007B		SGI			$6,755.75
0007C		Classified			$2,702.30
0008	**Section 8.4**	**Continuous Monitoring Support**	**EA**		
0008A		Annual Security Controls Test	(b)(4)		$252,000.00
0008B		Continuous Monitoring Activities for a Small System (Less than 15 components) -Low Sensitivity			$90,323.01
0008C		Continuous Monitoring Activities for a Small system (Less than 15 components) - Moderate Sensitivity			$158,187.35
0008D		Continuous Monitoring Activities for a Medium system (16-50 components) - Moderate Sensitivity			$229,088.25
0008E		Continuous Monitoring Activities for a Medium system (16-50 components) - High Sensitivity			$147,607.95
0008F		Continuous Monitoring Activities for a Large system (51-199 components) - Moderate Sensitivity			$49,809.45
0008G		Continuous Monitoring Activities for a Large system (51-199 components) - High Sensitivity			$174,615.15
0009	**Section 8.4**	**Continuous Monitoring Support**	**HR**		
0009A		Security Engineering Support	(b)(4)		$282,034.56
		Information Assurance/Security Specialist (Entry Level)			
		Information Assurance/Security Specialist (Journeyman)			
		Information Assurance/Security Specialist (Senior)			
		Information Assurance/Security Specialist (Master)			
		Technical Writer			
0009B		Process Support			$190,011.60
		Information Assurance/Security Specialist (Master)			
0010	**Section 8.5**	**Data Calls**	**HR**		
			(b)(4)		$25,057.20
		Information Assurance/Security Specialist (Entry Level)			
0011	**Section 8.6.1**	**Incident Response**	**HR**		
			(b)(4)		$214,414.00
		Subject Matter Expert (Senior)			
0012	**Section 8.6.2**	**Security Architecture**	**HR**		
			(b)(4)		$153,070.20
		Computer Forensic and Intrusion Analyst			
		Subject Matter Expert (Master)			

4.8.3 CSPSS Option 7 Cost/Price – Part 3

Option 7: August 31, 2019 - August 30, 2020					
Contract Line Item Number (CLIN)	SOW Cross Reference	Description and GSA Alliant Small Business GWAC Labor Category	Unit Total	Unit Price	Ceiling Price
0013	**Section 8.6.3**	**Vulnerability Assessment**	**EA**		
0013A		Small system (Less than 15 components)	(b)(4)		$18,000.00
0013B		Medium system (16-50 components)			$63,660.64
0013C		Large system (51-199 components)			$50,798.08
0014	**Section 8.6.4**	**Source Code Reviews**	**HR**		
			(b)(4)		$52,476.00
		Subject Matter Expert (Master)			
0015	**Section 8.6.5**	**Penetration Testing**	**HR**		
			(b)(4)		$80,585.60
		Information Assurance/Security Specialist (Journeyman)			
		Subject Matter Expert (Senior)			
		Subject Matter Expert (Master)			
		Technical Writer			
0016	**Section 8.6.6**	**Security Impact Assessments**	**EA**		
0016A		Small system (Less than 10 components tested)	(b)(4)		$43,500.00
0016B		Medium system (11-60 components tested)			$77,885.52
0016C		Large system (60-120 components tested)			$33,626.36
0017	**Section 8.7.1**	**Cyber Security Policy**	**HR**		
			(b)(4)		$47,862.00
		Subject Matter Expert (Journeyman)			
		Technical Writer			
0018	**Section 8.7.2**	**Processes, Procedures, Templates, Checklists, Standards, and Guidance**	**HR**		
			(b)(4)		$75,500.50
		Information Assurance/Security Specialist (Journeyman)			
		Subject Matter Expert (Master)			
		Technical Writer			
0019	**Section 8.7.7**	**Communications**	**HR**		
			(b)(4)		$59,743.20
		Information Assurance/Security Specialist (Entry Level)			
		Subject Matter Expert (Master)			
		Technical Writer			
1020	**N/A**	**Other Direct Costs (Not to Exceed)**	N/A	N/A	$160,000.00

Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this proposal.

4.8.4 CSPSS Option 7 Cost/Price – Part 4

Option 7: August 31, 2019 - August 30, 2020 [OPTIONAL CLINs]					
Contract Line Item Number (CLIN)	SOW Cross Reference	Description and GSA Alliant Small Business GWAC Labor Category	Unit Total	Unit Price	Ceiling Price
0021	Section 8.2.1	**Residual Risk per system**	HR		
		Special systems (infrastructure)	(b)(4)		$77,671.40
		Information Assurance/Security Specialist (Entry Level)			
		Information Assurance/Security Specialist (Journeyman)			
		Information Assurance/Security Specialist (Master)			
		Subject Matter Expert (Master)			
		Technical Writer			
0022	Section 8.3.1	**Authorization**	HR		
		Special system (At least 200 components)	(b)(4)		$117,296.84
		Information Assurance/Security Specialist (Entry Level)			
		Information Assurance/Security Specialist (Senior)			
		Information Assurance/Security Specialist (Master)			
		Quality Assurance Specialist (Journeyman)			
		Technical Writer			
0023	Section 8.4	**Continuous Monitoring Support**	HR		
		Special system (At least 200 components)	(b)(4)		$108,062.52
		Information Assurance/Security Specialist (Entry Level)			
		Information Assurance/Security Specialist (Journeyman)			
		Information Assurance/Security Specialist (Master)			
		Quality Assurance Specialist (Journeyman)			
		Subject Matter Expert (Senior)			
		Technical Writer			
0024	Section 8.6.3	**Vulnerability Assessment**	HR		
		Special system (At least 200 components)	(b)(4)		$72,122.64
		Information Assurance/Security Specialist (Journeyman)			
		Information Assurance/Security Specialist (Senior)			
		Information Assurance/Security Specialist (Master)			
		Quality Assurance Specialist (Journeyman)			
		Technical Writer			
0025	Section 8.6.6	**Security Impact Assessments**	HR		
		Special system (121 or more components tested)	(b)(4)		$59,471.60
		Information Assurance/Security Specialist (Entry Level)			
		Information Assurance/Security Specialist (Master)			
		Quality Assurance Specialist (Journeyman)			
		Technical Writer			
0026	Section 8.7.3	**Cyber Security Relevant Business Solutions**	HR		
			(b)(4)		$84,150.00
		Information Assurance/Security Specialist (Journeyman)			
		Subject Matter Expert (Master)			
		Technical Writer			

4.8.5 CSPSS Option 7 Cost/Price – Part 5

Option 7: August 31, 2019 - August 30, 2020 [OPTIONAL CLINs]					
Contract Line Item Number (CLIN)	SOW Cross Reference	Description and GSA Alliant Small Business GWAC Labor Category	Unit Total	Unit Price	Ceiling Price
0027	Section 8.7.4	**Cyber Security Awareness Training**	HR		
			(b)(4)		$27,049.20
		Information Assurance/Security Specialist (Entry Level)			
		Information Assurance/Security Specialist (Master)			
		Subject Matter Expert (Master)			
		Technical Writer			
0028	Section 8.7.5	**Cyber Security Role Based Awareness Training (development and instruction)**	EA		
		Course Development per day	(b)(4)		$63,987.04
0029	Section 8.7.5	**Cyber Security Role Based Awareness Training (development and instruction)**	HR		
		Instruction per day (42 days)	(b)(4)		$33,381.88
		Information Assurance/Security Specialist (Entry Level)			
		Information Assurance/Security Specialist (Master)			
		Subject Matter Expert (Senior)			
		Subject Matter Expert (Master)			
0030	Section 8.7.6	**Cyber Security Conference**	HR		
			(b)(4)		$52,339.30
		Information Assurance/Security Specialist (Journeyman			
		Information Assurance/Security Specialist (Master)			
		Subject Matter Expert (Master)			
				Total Without Optional CLINs	**$5,667,682.87**
				Total of Optional CLINs	**$695,532.42**
				Option 7 Grand Total	**$6,363,215.29**

4.9 CSPSS Option 8 (3 Months) Cost/Price

4.9.1 CSPSS Option 8 Cost/Price – Part 1

Option 8: August 31, 2020 - November 30, 2020					
Contract Line Item Number (CLIN)	SOW Cross Reference	Description and GSA Alliant Small Business GWAC Labor Category	Unit Total	Unit Price	Ceiling Price
0001	**Section 8.0**	**Overall Contract Responsibilities**	**HR**		
0001A		Financials and Status Reporting	(b)(4)		$56,075.70
		Administration/Clerical (Senior)			
		Financial Analyst			
0001B		Support for Scanning Laptops and Other Tools			$28,040.20
		Information Assurance/Security Specialist (Entry Level)			
0001C		Quality Assurance for Overall contract Only			$64,083.72
		Quality Assurance Specialist (Journeyman)			
		Subject Matter Expert (Senior)			
0002	**Section 8.1.2**	**Project Plan and Project Manager Support**	**HR**		
0002A		Project Manager	(b)(4)		$99,884.40
		Project Manager			
		Project Manager			
0002B		Program Manager			$12,391.00
		Program Manager			
0003	**Section 8.2.2**	**Classified Processing Support**	**HR**		
			(b)(4)		$16,480.92
		Information Assurance/Security Specialist (Entry Level)			
		Information Assurance/Security Specialist (Master)			
		Subject Matter Expert (Senior)			
0004	**Section 8.2.3**	**Evaluate New Technology**	**HR**		
			(b)(4)		$23,764.08
		Information Assurance/Security Specialist (Entry Level)			
		Subject Matter Expert (Master)			
0005	**Section 8.2.4**	**Best Practices**	**HR**		
			(b)(4)		$12,816.72
		Information Assurance/Security Specialist (Entry Level)			
		Subject Matter Expert (Master)			
		Technical Writer			
0006	**Section 8.3.1**	**Authorization**	**EA**		
0006A		Small system (Less than 15 components) -Low Sensitivity	(b)(4)		$32,869.30
0006B		Small system (Less than 15 components) - Moderate Sensitivity			$89,496.96
0006C		Medium system (16-50 components) - Moderate Sensitivity			$108,443.92
0006D		Medium system (16-50 components) - High Sensitivity			$63,914.58
0006E		Large system (51-199 or greater components) - Moderate Sensitivity			$74,621.14
0006F		Large system (51-199 or greater components) - High Sensitivity			$80,497.10

4.9.2 CSPSS Option 8 Cost/Price – Part 2

Option 8: August 31, 2020 - November 30, 2020					
Contract Line Item Number (CLIN)	**SOW Cross Reference**	**Description and GSA Alliant Small Business GWAC Labor Category**	**Unit Total**	**Unit Price**	**Ceiling Price**
0007	**Section 8.3.2**	**Laptop Authorization**	**EA**		
0007A		General Use	(b)(4)		$2,702.30
0007B		SGI			$1,621.38
0007C		Classified			$810.69
0008	**Section 8.4**	**Continuous Monitoring Support**	**EA**		
0008A		Annual Security Controls Test	(b)(4)		$70,000.00
0008B		Continuous Monitoring Activities for a Small System (Less than 15 components) -Low Sensitivity			$30,107.67
0008C		Continuous Monitoring Activities for a Small system (Less than 15 components) - Moderate Sensitivity			$31,637.47
0008D		Continuous Monitoring Activities for a Medium system (16-50 components) - Moderate Sensitivity			$45,817.65
0008E		Continuous Monitoring Activities for a Medium system (16-50 components) - High Sensitivity			$49,202.65
0008F		Continuous Monitoring Activities for a Large system (51-199 components) - Moderate Sensitivity			$49,809.45
0008G		Continuous Monitoring Activities for a Large system (51-199 components) - High Sensitivity			$58,205.05
0009	**Section 8.4**	**Continuous Monitoring Support**	**HR**		
0009A		Security Engineering Support	(b)(4)		$70,959.20
		Information Assurance/Security Specialist (Entry Level)			
		Information Assurance/Security Specialist (Journeyman			
		Information Assurance/Security Specialist (Senior)			
		Information Assurance/Security Specialist (Master)			
		Technical Writer			
0009B		Process Support			$47,502.90
		Information Assurance/Security Specialist (Master)			
0010	**Section 8.5**	**Data Calls**	**HR**		
			(b)(4)		$6,264.30
		Information Assurance/Security Specialist (Entry Level)			
0011	**Section 8.6.1**	**Incident Response**	**HR**		
			(b)(4)		$53,603.50
		Subject Matter Expert (Senior)			
0012	**Section 8.6.2**	**Security Architecture**	**HR**		
			(b)(4)		$38,267.55
		Computer Forensic and Intrusion Analyst			
		Subject Matter Expert (Master)			

4.9.3 CSPSS Option 8 Cost/Price – Part 3

Option 8: August 31, 2020 - November 30, 2020					
Contract Line Item Number (CLIN)	SOW Cross Reference	Description and GSA Alliant Small Business GWAC Labor Category	Unit Total	Unit Price	Ceiling Price
0013	**Section 8.6.3**	**Vulnerability Assessment**	**EA**		
0013A		Small system (Less than 15 components)	(b)(4)		$18,000.00
0013B		Medium system (16-50 components)			$63,660.64
0013C		Large system (51-199 components)			$50,798.08
0014	**Section 8.6.4**	**Source Code Reviews**	**HR**		
			(b)(4)		$13,119.00
		Subject Matter Expert (Master)			
0015	**Section 8.6.5**	**Penetration Testing**	**HR**		
			(b)(4)		$20,046.10
		Information Assurance/Security Specialist (Journeyman)			
		Subject Matter Expert (Senior)			
		Subject Matter Expert (Master)			
		Technical Writer			
0016	**Section 8.6.6**	**Security Impact Assessments**	**EA**		
0016A		Small system (Less than 10 components tested)	(b)(4)		$14,500.00
0016B		Medium system (11-60 components tested)			$25,961.84
0016C		Large system (60-120 components tested)			$33,626.36
0017	**Section 8.7.1**	**Cyber Security Policy**	**HR**		
			(b)(4)		$11,965.50
		Subject Matter Expert (Journeyman)			
		Technical Writer			
0018	**Section 8.7.2**	**Processes, Procedures, Templates, Checklists, Standards, and Guidance**	**HR**		
			(b)(4)		$18,940.72
		Information Assurance/Security Specialist (Journeyman)			
		Subject Matter Expert (Master)			
		Technical Writer			
0019	**Section 8.7.7**	**Communications**	**HR**		
			(b)(4)		$14,935.80
		Information Assurance/Security Specialist (Entry Level)			
		Subject Matter Expert (Master)			
		Technical Writer			
1020	**N/A**	**Other Direct Costs (Not to Exceed)**	N/A	N/A	$40,000.00

Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this proposal.

4.9.4 CSPSS Option 8 Cost/Price – Part 4

Option 8: August 31, 2020 - November 30, 2020 [OPTIONAL CLINs]					
Contract Line Item Number (CLIN)	SOW Cross Reference	Description and GSA Alliant Small Business GWAC Labor Category	Unit Total	Unit Price	Ceiling Price
0021	Section 8.2.1	**Residual Risk per system**	HR		
		Special systems (infrastructure)	(b)(4)		$19,417.85
		Information Assurance/Security Specialist (Entry Level)			
		Information Assurance/Security Specialist (Journeyman)			
		Information Assurance/Security Specialist (Master)			
		Subject Matter Expert (Master)			
		Technical Writer			
0022	Section 8.3.1	**Authorization**	HR		
		Special system (At least 200 components)	(b)(4)		$29,296.85
		Information Assurance/Security Specialist (Entry Level)			
		Information Assurance/Security Specialist (Senior)			
		Information Assurance/Security Specialist (Master)			
		Quality Assurance Specialist (Journeyman)			
		Technical Writer			
0023	Section 8.4	**Continuous Monitoring Support**	HR		
		Special system (At least 200 components)	(b)(4)		$27,052.35
		Information Assurance/Security Specialist (Entry Level)			
		Information Assurance/Security Specialist (Journeyman)			
		Information Assurance/Security Specialist (Master)			
		Quality Assurance Specialist (Journeyman)			
		Subject Matter Expert (Senior)			
		Technical Writer			
0024	Section 8.6.3	**Vulnerability Assessment**	HR		
		Special system (At least 200 components)	(b)(4)		$18,083.44
		Information Assurance/Security Specialist (Journeyman)			
		Information Assurance/Security Specialist (Senior)			
		Information Assurance/Security Specialist (Master)			
		Quality Assurance Specialist (Journeyman)			
		Technical Writer			
0025	Section 8.6.6	**Security Impact Assessments**	HR		
		Special system (121 or more components tested)	(b)(4)		$14,867.90
		Information Assurance/Security Specialist (Entry Level)			
		Information Assurance/Security Specialist (Master)			
		Quality Assurance Specialist (Journeyman)			
		Technical Writer			
0026	Section 8.7.3	**Cyber Security Relevant Business Solutions**	HR		
			(b)(4)		$21,037.50
		Information Assurance/Security Specialist (Journeyman)			
		Subject Matter Expert (Master)			
		Technical Writer			

4.9.5 CSPSS Option 8 Cost/Price – Part 5

Option 8: August 31, 2020 - November 30, 2020 [OPTIONAL CLINs]					
Contract Line Item Number (CLIN)	**SOW Cross Reference**	**Description and GSA Alliant Small Business GWAC Labor Category**	**Unit Total**	**Unit Price**	**Ceiling Price**
0027	**Section 8.7.4**	**Cyber Security Awareness Training**	**HR**		
			(b)(4)		$6,762.30
		Information Assurance/Security Specialist (Entry Level)			
		Information Assurance/Security Specialist (Master)			
		Subject Matter Expert (Master)			
		Technical Writer			
0028	**Section 8.7.5**	**Cyber Security Role Based Awareness Training (development and instruction)**	**EA**		
		Course Development per day	(b)(4)		$15,996.76
0029	**Section 8.7.5**	**Cyber Security Role Based Awareness Training (development and instruction)**	**HR**		
		Instruction per day (42 days)	(b)(4)		$8,463.68
		Information Assurance/Security Specialist (Entry Level)			
		Information Assurance/Security Specialist (Master)			
		Subject Matter Expert (Senior)			
		Subject Matter Expert (Master)			
0030	**Section 8.7.6**	**Cyber Security Conference**	**HR**		
			(b)(4)		$13,111.41
		Information Assurance/Security Specialist (Journeyman)			
		Information Assurance/Security Specialist (Master)			
		Subject Matter Expert (Master)			
				Total Without Optional CLINs	**$1,645,445.54**
				Total of Optional CLINs	**$174,090.04**
				Option 8 Grand Total	**$1,819,535.58**

4.10 CSPSS Cost/Price Summary for Base and Options

CSPSS Cost Summary (August 31, 2012 – November 30, 2020)			
Year	Total Without Optional CLINs	Total of Optional CLINs	Total Per Year
Base Period: August 31, 2012 - August 30, 2013	$5,619,691.81	$683,112.94	$6,302,804.75
Option 1: August 31, 2013 - August 30, 2014	$5,619,691.81	$683,112.94	$6,302,804.75
Option 2: August 31, 2014 - August 30, 2015	$5,619,691.81	$683,112.94	$6,302,804.75
Option 3: August 31, 2015 - August 30, 2016	$5,643,563.14	$689,287.08	$6,332,850.22
Option 4: August 31, 2016 - August 30, 2017	$5,643,563.14	$689,287.08	$6,332,850.22
Option 5: August 31, 2017 - August 30, 2018	$5,667,682.87	$695,532.42	$6,363,215.29
Option 6: August 31, 2018 - August 30, 2019	$5,667,682.87	$695,532.42	$6,363,215.29
Option 7: August 31, 2019 - August 30, 2020	$5,667,682.87	$695,532.42	$6,363,215.29
Option 8: August 31, 2020 - November 30, 2020	$1,645,445.54	$174,090.04	$1,819,535.58
		GRAND TOTAL	$52,483,296.14

ATTACHMENT 1 – MAR, INCORPORATED'S GSA ALLIANT SMALL BUSINESS CONTRACT WITH MODIFICATIONS

RFP Section E.9, pages 5

The following pages contain MAR's GSA Alliant Small Business Contract with modifications.

SOLICITATION, OFFER AND AWARD

1. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)	RATING	PAGE OF PAGES
		1 | 1

2. CONTRACT NUMBER	3. SOLICITATION NUMBER	4. TYPE OF SOLICITATION	5. DATE ISSUED
GS00Q08BND0050	TQ2006MCB0002	☐ SEALED BID (IFB) ☒ NEGOTIATED (RFP)	9/29/06

7. ISSUED BY	CODE	8. ADDRESS OFFER TO *(If other than Item 7)*
U.S. General Services Administration Small Business GWAC Center – Alliant SB 1500 E. Bannister Road, Kansas City, MO 64131		Same Block 7

NOTE: In sealed bid solicitations "offer" and "offeror" mean "bid" and "bidder"

SOLICITATION

9. Sealed offers in original for furnishing the supplies or services in the Schedule will be received at the place specified in Item 8, or if hand carried, in the depository located in (See Block 7) until 1:30 PM CST local time.

CAUTION ! LATE Submissions, Modifications, and Withdrawals: See Section L, Provision No. 52.214-7 or 52.215-1. All offers are subject to all terms and conditions contained in this solicitation.

Amdt 0002: December 6, 2006 1:30 PM

10. FOR INFORMATION CALL:	A. NAME	B. TELEPHONE *(NO COLLECT CALLS)* AREA CODE	NUMBER	EXT.	C. E-MAIL ADDRESS
	Mary Catherine Beasley				sbgwac@gsa.gov

11. TABLE OF CONTENTS

(X)	SEC.	DESCRIPTION	PAGE(S)	(X)	SEC.	DESCRIPTION	PAGE(S)
		PART I - THE SCHEDULE				PART II - CONTRACT CLAUSES	
X	A	SOLICITATION/CONTRACT FORM	1	X	I	CONTRACT CLAUSES	17
X	B	SUPPLIES OR SERVICES AND PRICE/COST	6			PART III - LIST OF DOCUMENTS, EXHIBITS AND OTHER ATTACH.	
X	C	DESCRIPTION/SPECS./WORK STATEMENT	11	X	J	LIST OF ATTACHMENTS	1
X	D	PACKAGING AND MARKING	1			PART IV - REPRESENTATIONS AND INSTRUCTIONS	
X	E	INSPECTION AND ACCEPTANCE	1	X	K	REPRESENTATIONS, CERTIFICATIONS AND OTHER STATEMENTS OF OFFERORS	3
X	F	DELIVERIES OR PERFORMANCE	2				
X	G	CONTRACT ADMINISTRATION DATA	9	X	L	INSTRS., CONDS., AND NOTICES TO OFFERORS	24
X	H	SPECIAL CONTRACT REQUIREMENTS	11	X	M	EVALUATION FACTORS FOR AWARD	9

OFFER *(Must be fully completed by offeror)*

NOTE: Item 12 does not apply if the solicitation includes the provisions at 52.214-16, Minimum Bid Acceptance Period.

12. In compliance with the above, the undersigned agrees, if this offer is accepted within 365 calendar days *(60 calendar days unless a different period is inserted by the offeror)* from the date for receipt of offers specified above, to furnish any or all items upon which prices are offered at the price set opposite each item, delivered at the designated point(s), within the time specified in the schedule.

13. DISCOUNT FOR PROMPT PAYMENT *(See Section I, Clause No. 52.232-8)*	10 CALENDAR DAYS %	20 CALENDAR DAYS %	30 CALENDAR DAYS %	CALENDAR DAYS %

14. ACKNOWLEDGMENT OF AMENDMENTS *(The offeror acknowledges receipt of amendments to the SOLICITATION for offerors and related documents numbered and dated):*	AMENDMENT NO.	DATE	AMENDMENT NO.	DATE
	0001	11/2/06		
	0002	11/7/06		
	0003	11/9/06		

15A. NAME AND ADDRESS OF OFFEROR	CODE 2F821	FACILITY	16. NAME AND TITLE OF PERSON AUTHORIZED TO SIGN OFFER *(Type or print)*
MAR, Incorporated 1803 Research Blvd, Ste 204 Rockville, MD 20850			Michael P. Norcio Chairman and CEO

15B. TELEPHONE NUMBER AREA CODE	NUMBER	EXT.	15C. ☐ CHECK IF REMITTANCE ADDRESS IS DIFFERENT FROM ABOVE - ENTER SUCH ADDRESS IN SCHEDULE.	17. SIGNATURE	18. OFFER DATE
301	230	4576			12/06/2006

AWARD *(To be completed by Government)*

19. ACCEPTED AS TO ITEMS NUMBERED	20. AMOUNT	21. ACCOUNTING AND APPROPRIATION
MINIMUM GUARANTEE	$2500.00	2007.2008.255F.FD2H.00.F0DY0000.FD957.516

22. AUTHORITY FOR USING OTHER THAN FULL AND OPEN COMPETITION: ☐ 10 U.S.C. 2304(c)( ) ☐ 41 U.S.C. 253(c)( )	SUBMIT INVOICES TO ADDRESS SHOWN on Task Orders	ITEM

24. ADMINISTERED BY *(If other than Item 7)* CODE	25. PAYMENT WILL BE MADE BY CODE
SAME AS BLOCK 7	DESIGNATED ON ORDERS

26. NAME OF CONTRACTING OFFICER *(Type or print)*	27. UNITED STATES OF AMERICA	28. AWARD DATE
GREG D. BYRD		2-8-07

IMPORTANT – Award will be made on this Form, or on Standard Form 26, or by other authorized official written notice.

AUTHORIZED FOR LOCAL REPRODUCTION
Previous edition is unusable

STANDARD FORM 33 (Rev. 9-97)
Prescribed by GSA – FAR (48 CFR) 53.214(

SECTION B
SUPPLIES OR SERVICES AND PRICES/COSTS

B.1 GENERAL

The Alliant Small Business (SB) Governmentwide Acquisition Contract (Alliant SB GWAC) is a Multiple Award, Indefinite Delivery, Indefinite Quantity contract to provide information technology solutions through performance of a broad range of services which may include the integration of various technologies critical to the services being acquired.

The Contractor shall provide all management, supervision, labor, facilities and materials necessary to perform on a task order basis.

Hereafter, the Alliant SB GWAC will be referred to as the "Basic Contract" while task orders issued under the Basic Contract will be referred to as "Order(s)".

B.2 AUTHORITY

The Office of Management and Budget has designated the U.S. General Services Administration (GSA) as an Executive Agent for Governmentwide information technology (IT) acquisitions pursuant to Section 5112(e) of the Clinger-Cohen Act, 40 U.S.C. 11302(e).

The scope of this designation includes the award and administration of the Basic Contract and delegation of authority for the award and administration of the Orders as set forth in Section G.2.

The authority of the Procuring Contracting Officer (PCO), the Administrative Contracting Officer (ACO) and the Ordering Contracting Officer (OCO) are defined in Section G.3.

B.3 ECONOMY ACT

In accordance with FAR 17.500(b)(2), the Economy Act does not apply to acquisitions using Governmentwide acquisition contracts.

B.4 MAXIMUM PROGRAM CEILING AND MINIMUM CONTRACT GUARANTEE

Pursuant to FAR 16.504(a), the total maximum quantity of all supplies and services under the Basic Contract (for all awardees combined) shall not exceed $15 Billion, including the Option.

The total minimum quantity, guaranteed by the Government, is $2,500 for each awardee.

B.5 CONTRACT ACCESS FEE

The Contract Access Fee (CAF) is ¾ of a percent (i.e., 0.0075) to be applied to the total price/cost for contractor performance as billed to the Government.

The formula is: Total CAF = Total Price or Costs * CAF Percentage.

The total CAF collected per Order will be capped at a set amount to be determined by the Alliant GWAC Program Office. For more information on this cap, please see the Alliant website (http://www.gsa.gov/alliant).

On all Orders, regardless of Order type, Contractors must estimate CAF in their proposals and OCOs may fund CAF as a separate Contract Line Item Number (CLIN). On Labor-Hour type Orders, OCOs may require Contractors to include CAF in their Loaded Hourly Labor Rate.

The Contractor remits the CAF to GSA in accordance with Section G.9.5.

B.6 ORDER TYPES

As defined in FAR Part 16, Type of Contracts, all types of Fixed-Price, Cost-Reimbursement, Incentive, Time-and-Materials (T&M), and Labor-Hour (L-H) are permissible for Orders under the Basic Contract. In addition, the Award Term Incentive may be used for Orders under the Basic Contract.

Indefinite Delivery, Indefinite Quantity, Blanket Purchase Agreements, and Letter Contracts are not permissible Order types under the Basic Contract.

Orders may be multi-year and/or include options as defined in FAR Part 17 and agency-specific FAR Part 17 supplements.

B.6.1 Order Type Preference

The OCO should determine the Order type using the following order of precedence:

(1) Fixed-Price (all types)
(2) Cost-Reimbursement (all types)
(3) T&M or L-H

Pursuant to FAR 16.601(c), T&M and L-H Orders require a Determination and Findings (D&F) by the OCO that no other Order type is suitable.

B.6.2 Performance Based Preference

Pursuant to FAR 37.102(a)(2), the OCO should use performance-based acquisition methods to the maximum extent practicable using the following order of precedence:

(1) A Firm-Fixed Price Performance-Based Order;
(2) A Performance-Based Order that is not Firm-Fixed Price;
(3) An Order that is not Performance-Based.

B.7 ORDER PRICING (ALL ORDER TYPES)

The OCO is responsible for the determination of cost or price reasonableness for each Order type. When adequate price competition exists (see FAR 15.403-1(b)(1)), generally no additional information is necessary to determine the reasonableness of cost or price. If adequate price competition does not exist and no other exceptions apply (see FAR 15.403-1(b)), the OCO must request a Certificate of Current Cost and Pricing Data in accordance with FAR 15.403-4.

If a Contractor does not have an approved purchasing system, the Contractor shall request and receive OCO consent to subcontract in accordance with FAR 44.2 Consent to Subcontracts, and FAR 52.244-2, Subcontracts.

B.7.1 Fixed Price

The OCO must determine fair and reasonable pricing for all Fixed-Price Orders in accordance with FAR 15.4, Pricing, and FAR 16.2, Fixed-Price Contracts.

B.7.2 Cost Reimbursement

The OCO must determine fair and reasonable pricing, analyze and negotiate profit for all Cost-Reimbursement Orders, in accordance with FAR 15.4, Pricing, and FAR 16.3, Cost-Reimbursement Contracts.

Contractors are required to have an adequate cost accounting system for Cost Reimbursable type Orders in accordance with FAR 16.301-3(a)(1). Contractors will be required to submit a cost proposal with supporting information for each cost element, including, but not limited to, Direct Labor, Fringe Benefits, Overhead, General and Administrative (G&A) expenses, Facilities Capital Cost of Money, Other Direct Costs, and Profit consistent with their cost accounting system, provisional billing rates, and forward pricing rate agreements.

The Government will reimburse the Contractor for all reasonable, allowable, and allocable costs in accordance with FAR 31, Contract Cost Principles and Procedures.

B.7.3 Incentive

The OCO must determine fair and reasonable pricing for all Incentive Orders and develop a plan to implement and monitor an Award-Fee, Incentive-Fee, or Award-Term result in accordance with FAR 15.4, Pricing, and FAR 16.4, Incentive Contracts.

B.7.4 Time and Materials and Labor-Hour

To be considered eligible for award, the Contracting Officer determined that the evaluated price of the offeror was fair and reasonable. Section J, Attachments 2 (Government Site) and 3 (Contractor Site) of the Basic Contract provide competitive Loaded Hourly Labor Rates within CONUS for T&M and L-H type Orders only. The OCO is responsible for considering the level of effort and the mix of labor proposed to perform a specific task being ordered, and for determining that the total price for the task order is reasonable.

The OCO is authorized to establish different hourly rates suited to meet the ordering agency's specific requirements and determine fair and reasonable pricing in accordance with FAR 15.4, Pricing, and FAR 16.601 Time and Materials Contracts when other considerations, such as geographic location or security clearances require deviation from established pricing.

Contractors shall explain in their Order proposals any Loaded Hourly Labor Rates that exceed the rates in the Basic Contract. Upon request of the OCO, the Contractor shall provide other than cost or pricing data, to include, a cost element breakdown of each Loaded Hourly Labor Rate, including Profit, in accordance with the Contractor's cost accounting system, as well as any other supporting information the OCO deems necessary.

B.7.4.1 Payment and Proposal Requirements on T&M and L-H Orders

For payments on T&M/L-H Orders, Contractors are subject to FAR 52.232-7 Payments Under Time-and-Materials and Labor-Hour Contracts.

For proposal requirements on T&M/L-H Orders, the OCO must determine one of the following conditions and include the appropriate provision in each T&M and L-H Order solicitation:

With Adequate Price Competition:

(1) Pursuant to FAR 52.216-29, if price is expected to be based on adequate price competition, the Contractor must provide "separate and/or blended" Loaded Hourly Labor Rates for Prime contractor labor, each Subcontractor, and/or each Division, Subsidiary, or Affiliate. The Contractor must specify whether each Loaded Hourly Labor Rate applies to the Prime contractor, each Subcontractor, and/or each Division, Subsidiary or Affiliate.

(2) For the Department of Defense, pursuant to FAR 52.216-29 with DFARs 252.216-7002, Alternate A, if price is expected to be based on adequate price competition, the Contractor must only provide "separate" Loaded Hourly Labor Rates for Prime Contractor labor, each Subcontractor, and/or each Division, Subsidiary, or Affiliate. The Contractor must specify whether each Loaded Hourly Labor Rate applies to the Prime contractor, each Subcontractor, and/or each Division, Subsidiary or Affiliate.

Without Adequate Price Competition:

Pursuant to FAR 52.216-30, if price is not expected to be based on adequate price competition, the Contractor must identify and provide "separate" Loaded Hourly Labor Rates for Prime contractor labor, each Subcontractor, and/or each Division, Subsidiary, or Affiliate.

Commercial Items:

Pursuant to FAR 52.216-31, if price is expected to be based on commercial items, separate Loaded Hourly Labor Rates are not required for Prime contractor labor, each Subcontractor, and/or Affiliate labor. The Contractor must specify fixed hourly rates in its offer that include wages, overhead, general and administrative expenses, and profit. The Contractor must specify whether the fixed hourly rate for each labor category applies to labor performed by the Prime Contractors, each Subcontractor, and/or each Division, Subsidiary, or Affiliate.

B.7.4.2 Materials on T&M Orders

Refer to FAR Clause 52.232-7 Payments Under Time-and-Materials and Labor Hour Contracts (Feb 2007)

The OCO must identify a not-to-exceed materials ceiling under a separate CLIN on the Order.

B.7.4.3 Indirect Costs Under T&M Orders

Refer to FAR Clause 52.232-7 Payments Under Time-and-Materials and Labor Hour Contracts (Feb 2007)

B.8 TRAVEL PRICING (ALL ORDER TYPES)

Travel will be reimbursed at actual cost in accordance with the limitations set forth in FAR 31.205-46.

Profit shall not be applied to travel costs. Contractors may apply indirect costs to travel in accordance with the Contractor's usual accounting practices consistent with FAR 31.2.

The OCO must identify a not-to-exceed travel ceiling under a separate CLIN on the Order.

B.9 LABOR SUBJECT TO THE DAVIS BACON ACT

To the extent that construction, alteration and repair are subject to the Davis Bacon Act and within scope of an Order and the Basic Contract, the OCO must identify such work under a separate CLIN on the Order and apply wages in accordance with FAR 22.4, Davis Bacon Act Wage Determinations.

Any construction, alteration and repair shall be firm fixed price, even if other aspects of the Order are another Order type.

The Basic Contract does not include all applicable flow-down clauses for labor categories subject to the Davis Bacon Act. Each Order must be tailored to include the appropriate clauses.

B.10 LABOR SUBJECT TO THE SERVICE CONTRACT ACT (SCA)

The Basic Contract's labor categories are considered bona fide executive, administrative, professional labor and generally exempt from the SCA.

To the extent that any labor is subject to the SCA and within scope of an Order and the Basic Contract, the OCO must identify such work under a separate CLIN on the Order and apply wages in accordance with FAR 22.10, Service Contract Act Wage Determinations.

The Basic Contract does not include all applicable flow-down clauses for labor categories subject to the Service Contract Act. Each Order must be tailored to include the appropriate clauses.

B.11 LABOR OUTSIDE THE CONTINENTAL UNITED STATES (OCONUS)

"OCONUS" is defined as other than the 48 contiguous states plus the District of Columbia.

It is anticipated that there may be Orders for work OCONUS. The U.S. Department of State's Bureau of Administration, Office of Allowances, (http://www.state.gov/m/a/als/), publishes quarterly report indexes of living costs abroad, per-diem rate maximums, quarter's allowances, hardship differentials, and danger pay allowances.

The Department of State Standardized Regulations (DSSR) are the controlling regulations for allowances and benefits available to all U.S. Government civilians assigned to foreign areas; however, for Orders issued under the Basic Contract, Contractor civilians assigned to foreign areas shall not exceed the allowances and benefits in the DSSR as well.

For OCONUS Orders where costs are not specifically addressed in the DSSR, the Government will reimburse the Contractor for all reasonable, allowable, and allocable costs in accordance with FAR 31, Contract Cost Principles and Procedures.

(END OF SECTION B)

SECTION C
STATEMENT OF WORK

C.1 BACKGROUND

The Basic Contract will provide Federal government agencies with integrated Information Technology (IT) solutions for evolving needs on a global basis. Integrated IT solutions are comprised of some or all components described below in Section C.3, and may be tailored to meet agencies' mission needs. Work may be performed at headquarters and/or field offices located throughout the world, as specified in each Order, to provide a variety of IT solutions and support services, including new and emerging technologies that will evolve over the life of the Basic Contract.

C.2 SCOPE

The scope of the Basic Contract includes any and all components of an integrated IT solution, including all current and any new technologies which may emerge during the life cycle of the Basic Contract. In addition, the scope of the Basic Contract includes information technology systems and services in support of National Security Systems, as defined in FAR 39.002. The Basic Contract provides IT Solutions through performance of a broad range of services which may include the integration of various technologies critical to the services being acquired.

As the definition of IT changes over the lifecycle of the Basic Contract, the scope of the Basic Contract will be considered to coincide with the current definition at any given time.

C.2.1 Definition of Information Technology

Per Section C.1, definitions of Information Technology are provided as follows:

C.2.1.1 Clinger-Cohen Act

(a) The term 'information technology', with respect to an executive agency means any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which (i) requires the use of such equipment, or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product.

(b) The term 'information technology' includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.

(c) Notwithstanding subparagraphs (A) and (B), the term 'information technology' does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract.

C.2.1.2 Federal Acquisition Regulation (FAR)

The FAR defines information technology in section 2.101(b):

"Information technology" means any equipment, or interconnected system(s) or subsystem(s) of equipment, that is used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency.

(a) For purposes of this definition, equipment is used by an agency if the equipment is used by the agency directly or is used by a contractor under a contract with the agency that requires—(i) Its use; or (ii) To a significant extent, its use in the performance of a service or the furnishing of a product.

(b) The term "information technology" includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources.

(c) The term "information technology" does not include any equipment that— (i) Is acquired by a contractor incidental to a contract; or (ii) Contains imbedded information technology that is used as an integral part of the product, but the principal function of which is not the acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. For example, HVAC (heating, ventilation, and air conditioning) equipment, such as thermostats or temperature control devices, and medical equipment where information technology is integral to its operation, are not information technology.

C.3 COMPONENTS OF AN IT SOLUTION

The Contractor shall provide Infrastructure and related services, Applications and related services, and IT Management Services to support agencies' integrated IT solution requirements.

In order to provide a common framework for defining and understanding the components of an IT solution, this section will refer to terminology included in the Federal Enterprise Architecture (FEA) and Department of Defense Enterprise Architecture (DoDEA). More detailed information about FEA and DoDEA may be found in Section J, Attachment 5. Usage of this terminology or structure is not required within individual Orders placed on this contract.

The Contractor shall promote IT solutions that support Federal government operational requirements for standardized technology and application service components. This shall

facilitate integration requirements for broad Federal IT and E-Gov initiatives, as well as promote the sharing, consolidation, and "re-use" of business processes and systems across the Federal government. The Contractor shall promote the use of open source solutions and open technology development where practicable to enable this re-use.

Within each section below, an overview of the contract solution and service offerings is provided, followed by examples of work to be performed relative to Order requirements. Examples are not meant to be all-inclusive, but rather general indications of the types of products or services within a given category. Other products and services not listed as examples which adhere to the definition for each section are also within scope. For more detailed on information about the particular components of the FEA/DoDEA reference models listed below, see Section J, Attachment 5.

C.3.1 Infrastructure

Infrastructure serves as the foundation and building blocks of an integrated IT solution. It is the hardware which supports Application Services (C.3.2) and IT Management Services (C.3.3); the software and services which enable that hardware to function; and the hardware, software, and services which allow for secure communication and interoperability between all business and application service components.

Infrastructure services facilitate the development and maintenance of critical IT infrastructures required to support Federal government business operations. This section includes the technical framework components that make up integrated IT solutions. One or any combination of these components may be used to deliver IT solutions intended to perform a wide array of functions which allow agencies to deliver services to their customers (or users), whether internal or external, in an efficient and effective manner.

Infrastructure includes hardware, software, licensing, technical support, and warranty services from third party sources, as well as technological refreshment and enhancements for that hardware and software.

This section is aligned with the FEA/DoDEA Technical Reference Model (TRM) which describes these components using a vocabulary that is common throughout the entire Federal government. A detailed review of the TRM is provided in Section J, Attachment 5.

Infrastructure includes complete life cycle support for all hardware, software, and services represented above, including planning, analysis, research and development, design, development, integration and testing, implementation, operations and maintenance, information assurance, and final disposition of these components. The services also include administration and help desk functions necessary to support the IT infrastructure (e.g., desktop support, network administration).

Infrastructure components of an integrated IT solution can be categorized as follows:

C.3.1.1 Service Access and Delivery

These components are responsible for facilitating the end-to-end collection and distribution of data that is either entered or requested by a user. These components include all functions necessary to communicate in a client-server environment. Examples of these components include, but are not limited to, web browsers, Virtual Private Network (VPN), Remote Authentication Dial-In User Service (RADIUS), Peer-to-peer, Section 508 compliance, HyperText Transfer Protocol (HTTP), File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP).

C.3.1.2 Service Platform and Infrastructure

These components include all functions necessary for processing and storing data. These components provide and manage the resources available for Application Services (C.3.2). Examples of these components include, but are not limited to, desktops, laptops, servers, mainframes, routers, switches, printers, Asynchronous Transfer Mode (ATM), T1, Digital Subscriber Line (DSL), Ethernet, Windows/UNIX, Java/.NET; web server/portal; database, data storage, data warehouse; *software development tools*: testing, modeling, versioning, configuration management.

C.3.1.3 Component Framework

These components consist of the design of application or system software that incorporates interfaces for interacting with other programs and for future flexibility and expandability. These components define higher level logical functions to provide services in a way that is useful and meaningful to users and other Application Services (C.3.2). Examples of these components include, but are not limited to, digital certificates, biometrics; *business logic*: JavaScript, Visual Basic; *data interchange*: Simple Object Access Protocol (SOAP), Resource Description Framework (RDF); *data management*: Structured Query Language (SQL), Open DataBase Connectivity (ODBC), and OnLine Analytical Processing (OLAP).

C.3.1.4 Service Interface and Integration

These components define the discovery, interaction and communication technologies joining disparate systems and information providers. Application Services (C.3.2) leverage and incorporate these components to provide interoperability and scalability. Examples of these components include, but are not limited to: Messaging-Oriented Middleware (MOM), Object Request Broker (ORB), Enterprise Application Integration (EAI), EXtensible Markup Language (XML), Electronic Data Interchange (EDI), Web Services Description Language (WSDL), Universal Description, Discovery and Integration (UDDI).

C.3.2 Application Services

Application Services provide support for all applications and collaborative service capabilities. These services include support for developing and implementing enterprise and departmental-level applications. These applications may be "cross-cutting" in nature, with inter-related service processing components extending across/beyond the enterprise, or unique to a particular agency/department's mission requirements.

Application Services are aligned with the FEA/DoDEA Service Component Reference Model (SRM). The Contractor shall support all "service domains" outlined in the FEA SRM, to enable the advancement of business and performance objectives. These "service domains" identify the service capabilities required by Federal government agencies to support enterprise/departmental processes and applications.

The Contractor shall promote, to the maximum extent practicable use of commercially available technologies (e.g. Commercial Off-the-Shelf (COTS) and non-developmental items) to support Federal government agencies' IT solution requirements. The Contractor shall provide competencies to employ agencies' enterprise architectures (EAs) as required by individual Orders, to support IT solutions development and implementation and alignment with the FEA.

Application Services include complete life cycle support, including planning, analysis, research and development, design, development, integration and testing, implementation, operations and maintenance, information assurance, and final disposition.

In conjunction with the Application Services supporting each of the Service Domains defined in the FEA/DoDEA SRM, the Contractor shall provide Applications Services for systems required to support unique agency and departmental-level mission requirements, as specified in individual Orders. These services include support for existing and/or new/emerging mission requirements not yet served by the FEA model.

The following represents either components of applications or capabilities which Application Services will support. Each particular area includes, but is not limited to, support for the described functions.

C.3.2.1 Customer Services

Customer Relationship Management (CRM): All aspects of the CRM process, including planning, scheduling, and control activities involved with service delivery. The service components facilitate agencies' requirements for managing and coordinating customer interactions across multiple communication channels and business lines.

Customer Preferences: Customizing customer preferences relative to interface requirements and information delivery mechanisms (e.g., personalization, subscriptions, alerts and notifications).

Customer Initiated Services: Initiating service requests and seeking assistance from government agencies via online communication channels (e.g., online help, tutorials, self-service, reservation/registration, multilingual support, scheduling).

C.3.2.2 Process Automation

Tracking and Workflow: Automated routing, tracking, and management of documents (e.g., process tracking, case management, conflict resolution).

Routing and Scheduling: Automated distribution and scheduling activities (e.g., inbound/outbound correspondence management).

C.3.2.3 Business Management:

Process Management: Development and implementation of standard methodologies and automated process management systems, to facilitate agencies' requirements for managing and monitoring activities surrounding their core business operations (e.g., change management, configuration management, requirements management, program/project management, governance/policy management, quality management, risk management).

Organizational Management: Collaboration and communication activities (e.g., workgroup/groupware, network management).

Investment Management: Selecting, managing, and evaluating agencies' investments and capital asset portfolios (e.g., strategic planning/management, portfolio management, performance management).

Supply Chain Management: All aspects of supply chain management, from the initial sourcing phase through customer delivery (e.g., procurement, sourcing management, inventory management, catalog management, ordering/purchasing, invoice tracking, storefront/shopping cart, warehouse management, returns management, logistics/transportation).

C.3.2.4 Digital Asset Services

Content Management: Content development, maintenance, updates, and distribution (e.g., content authoring, content review/approval, tagging/aggregation, content publishing/delivery, syndication management).

Document Management: Capturing, indexing, and maintaining documents (e.g., document imaging, optical character recognition (OCR), document revisions, library/storage, review/approval, document conversion, indexing/classification).

Knowledge Management: Collecting and processing data from multiple sources and generating information to support business requirements (e.g., information retrieval, information mapping/taxonomy, information sharing, categorization, knowledge engineering, knowledge capture/distribution/delivery, smart documents).

Records Management: Administration of official government records (record linking/association, record storage/archival, document classification, document retirement, digital rights management).

C.3.2.5 Business Analytical Services

Analysis and Statistics: Applying analysis and statistics to examine/resolve business issues (e.g., mathematical, structural/thermal, radiological, forensics).

Visualization: Transforming data into graphical or image form (e.g., graphing/charting, imagery, multimedia, mapping/geospatial/elevation/global positioning systems (GPS), computer-aided design (CAD)).

Knowledge Discovery: Identifying and extracting information from multiple data source containing files stored in various formats (e.g., data mining, modeling, simulation).

Business Intelligence: Collecting information relevant to historical, existing, or future business needs (e.g., demand forecasting/management, balanced scorecard, decision support planning).

Reporting: Generating reports derived from single or multiple data sources (e.g., ad hoc reporting, standardized/canned reporting, OLAP).

C.3.2.6 Back Office Services

Data Management: Creating, using, processing, and managing data resources (e.g., data exchange, data mart, data warehouse, meta data management, data cleansing, extraction and transformation, data recovery). The data management services include support for agencies' use of the FEA/DoDEA Data Reference Model (DRM). For more information about the FEA/DoDEA DRM, see Section J, Attachment 5.

Human Resources: Recruitment, training, and management of government personnel (e.g., recruiting, career development/retention, time reporting, awards/benefit management, retirement management, education/training, travel management).

Financial Management: Government financing and accounting activities (e.g., billing and accounting, credit/charge, expense management, payroll, payment/settlement, debt collection, revenue management, internal controls, auditing, activity based management, currency translation).

Asset/Material Management: Acquisition and management of Federal government assets (property/asset management, asset cataloging/identification, asset transfer/allocation/maintenance, facilities management, computers/automation management).

Development and Integration: Development and integration of systems across diverse operating platforms (e.g., legacy integration, enterprise application integration, data integration, instrumentation/testing, software development).

Human Capital/Workforce Management Development and Integration: Planning and supervisory operations surrounding government personnel (e.g., resource planning/allocation, skills management, workforce directory/locator, team/organization management, contingent workforce management).

C.3.2.7 Support Services

Security Management: Assuring desired levels of protection for Federal systems, data, and related assets are achieved (e.g., identification/authentication, access control, encryption, intrusion detection, verification, digital signature, user management, role/privilege management, audit trail capture/analysis).

Collaboration: Communications, messaging, information sharing, scheduling and task management activities (e.g., email, threaded discussions, document library, shared calendaring, task management).

Search: Searching, querying, and retrieving data from multiple sources (e.g., precision/recall ranking, classification, pattern matching)

Communications: Voice, data, and video communications in multiple formats and protocols (e.g., real time chat, instant messaging, audio/video conferencing, event/news management, community management support, computer/telephony integration, voice communications).

Systems Management: All aspects of systems management (e.g., software distribution/license management, configuration/installation, remote systems control, enhancements/service updates, system resource monitoring, helpdesk support/issue tracking).

Forms Management: Creating, managing, and processing online forms to support business operations (e.g., forms creation, modification).

C.3.2.8 DoDEA Mission Area Support

The Alliant SB Basic Contract provides support for the DoDEA reference models relating DoD's specialized mission, business, and program areas. Though the DoDEA is an emerging standard, policy and procedures have been formalized for maintaining, evolving, and using the DoDEA reference models.

The DoDEA reference models leverage existing DoD standards and reflect the alignment with the FEA. The Alliant SB Basic Contract includes IT support services for DoD's Global Information Grid (GIG) architecture, Business, Warfighter, Intelligence, and Enterprise Information Environment (EIE) mission areas. More detailed information about DoDEA may be found in Section J, Attachment 5.

C.3.3 IT Management Services

IT Management Services provide support for operations and IT resource management requirements across the Federal government. These services encompass support for all strategic planning, management, and control functions integral to IT initiatives. The IT Management Services provide the foundational support to effectively align IT requirements with Federal government business operations.

IT Management Services provide support for all government lines of business, functions, and service components that comprise the FEA/DoDEA Performance Reference Model (PRM) and Business Reference Model (BRM). For more information about the PRM and BRM, see Section J, Attachment 5.

IT Management Services shall enable the development and implementation of enhanced governance capabilities, to efficiently and effectively support government agencies' mission requirements and service delivery operations. The services include, but shall not be limited to, support for the following functions:

C.3.3.1 Controls and Oversight

Development and implementation of management controls and systems required by agencies to evaluate, manage, and monitor program performance relative to IT initiatives (e.g., agency, program, and project-level performance plans for IT initiatives; performance measures to support evaluation and reporting requirements for IT initiatives in compliance with FEA/DoDEA PRM standards, etc.).

C.3.3.2 Risk Management and Mitigation

Identification of risk and preparation of risk management plans for IT projects, initiatives, and ongoing operations. Contingency planning to ensure continuity of IT operations and service recovery during emergency events (e.g., risk assessments to determine contingency planning requirements for IT operating environments; develop/maintain contingency, Continuity of Operations (COOP), and disaster recovery plans for IT components, develop/implement emergency preparedness systems).

C.3.3.3 Regulatory Development

Facilitate the development of IT policies, guidelines and standards to facilitate implementation of Federal laws and regulations. The services include support for development, implementation and maintenance of systems to support agencies' IT regulatory development, compliance, and enforcement activities (e.g., monitoring/ inspection/auditing of IT regulated activities to ensure compliance).

C.3.3.4 Planning and Resource Allocation

Facilitate the planning of IT investments, as well as determine and manage managing overall IT resources to efficiently and effectively support agencies' mission operations. This service area includes, but shall not be limited to support for the following functions:

Budget Formulation/Execution: Facilitate the integration of budgets and plans, at agency and departmental levels, to effectively link IT functions, activities, and resources with mission objectives.

Capital Planning: Facilitate the selection, management, and evaluation of IT investments relative to Federal government agencies' overall capital asset portfolios.

Enterprise Architecture (EA): Development and use of EA work products to manage current and future needs of Federal government business operations (i.e., "baseline" and "target" architectures). The services include transition planning and migration support for all EA components (e.g., business, information, application, and technology architectures), to advance the development and implementation of "core EA capabilities." The services shall provide support relative to Federal government mandates for measuring and reporting on the completion and usage of EA programs, as well as evaluating results for E-Gov alignment and implementation of Federal lines of business and other cross-governmental initiatives (e.g., SmartBUY, IPv6, HSPD-12).

Strategic Planning: Facilitate the effective alignment of IT requirements/ Information Resource Management (IRM) plans with strategic business plans and program initiatives.

Management Improvements: Development and implementation of improved systems and business practices to optimize productivity and service delivery operations (e.g., analysis, and implementation of improvements in the flow of IT work and program processes and tool utilization, including business system analysis, identification of requirements for streamlining, re-engineering, or re-structuring internal systems/business processes for improvement, determination of IT solution alternatives, benchmarking).

C.3.3.5 IT Security

Development and implementation of management, operational, and technical security controls required by agencies to assure desired levels of protection for IT systems and data are achieved (e.g., establishment of policy/procedures in support of Federal IT security requirements, conduct risk assessments to identify threats/vulnerabilities for existing/planned systems; support Federal mandates for measuring and reporting compliance, perform certification and accreditation (C&A) activities; provide training services to promote awareness and knowledge of compliance responsibilities for Federal IT security requirements).

C.3.3.6 System and Network Controls

Facilitate the planning, development, implementation, and management of system and network control mechanisms to support communication and automated needs. Facilitate the planning, organizing, coordinating, and controlling of the arrangement of the elements of protection and monitoring capabilities, and incident recovery actions of the information environment. The process takes configuration orders; status reports; and operational and functional performance requirements as inputs and provides performance capabilities and service and infrastructure controls as outputs.

System and network controls are controlled by environment standards such as policy and operational guidance. The service control requirements enable network controls and operational performance capabilities.

C.3.4 Ancillary Support

The Contractor shall provide ancillary support as necessary to offer an integrated IT solution. The ancillary support described here may only be included in an Order when it is integral to and necessary for the IT effort. Ancillary support may include, but is not limited to, such things as: clerical support; data entry; training; subject matter expertise; server racks, mounts, or similar items; and construction, alteration, and repair. A Contractor may propose a new or different skill level category when proposing Ancillary Support consistent with this Section, provided that the Contractor complies with all applicable contract clauses and labor laws, including the Service Contract Act or the Davis Bacon Act, as applicable.

C.3.4.1 Telecommunications/Wireless

Orders which include requirements for Telecommunications, Wireless, and Satellite products and services may be fulfilled under the Basic Contract scope, provided the work to be performed is part of a larger IT initiative. If the sole purpose of the task order is for phone/voice services provided over landline and/or wireless, i.e., federal/state tariffed phone service, then it would not be covered under the scope of this contract. Contractors are authorized to use government sources of supply in accordance with FAR 51.101 (i.e. Schedules, SATCOM, Networx...).

(END OF SECTION C)