PERFORMANCE WORK STATEMENT:
DOC CYBER SECURITY UNITY (CSU)

FOR
DOC OFFICE OF THE CIO
OFFICE OF CYBER SECURITY AND IT RISK MANAGEMENT (OCRM)
OFFICE OF THE SECRETARY

Table of Contents

1.0 BPA Overview

This is a non-personal services Blanket Purchase Agreement (BPA). The Government will not exercise any supervision or control over the service providers performing the services herein. Such service providers shall be accountable solely to the Contractor who, in turn is responsible to the Government as defined in this Performance Work Statement (PWS). The Contractor shall perform to the standards in this BPA.

2.0 Background

The position of the Chief Information Officer (CIO) was established by the Clinger- Cohen Act of 1996. The CIO implements the provisions of the Clinger-Cohen Act of 1996 and the Paperwork Reduction Act of 1995 regarding the acquisition, management, and use of information technology (IT) resources; manages Department of Commerce (DOC) compliance with the Computer Security Act of 1987, the Federal Information Security Modernization Act (FISMA) of 2014 (Public Law 113-283), Homeland Security Presidential Directive 7 of December 17, 2003, and implements the Office of Management and Budget Circular A-130, Management of Federal Information Resources. The CIO serves as the principal advisor to the Secretary on information resources and information systems management, and strives to improve the operations and services delivery of DOC's programs through the effective use of technology.

Among its duties, the Office of the CIO (OCIO) directs the following activities:

- Directs the computer security and critical infrastructure protection programs, which ensure the security of DOC systems by assisting operating units in identifying and implementing process controls for their sensitive and critical automated systems.
- Interprets and translates Federal laws, regulations, policies, and guidance to address agency-specific needs and in turn promulgates agency-wide IT policies, directives, and guidance and ensures compliance with those IT policies, directives and guidance. OCIO develops and promulgates the Department's IT Security Program Policy, which serves as a central repository for IT policy and guidance, including guidance and directives related to the sound management of IT Security.

The purpose of this statement of work is to obtain Contractor support in continuous operation and improvement of the current DOC enterprise-wide cybersecurity governance and oversight program.

2.1 Objective

This Statement of Work (SOW) describes a broad set of contractor responsibilities to support the program activities of the Office of Cyber Security and IT Risk Management (OCRM). The principal purpose of these responsibilities is to provide comprehensive expert cybersecurity support to the CIO and the Chief Information Security Officer (CISO) to:

- Provide cybersecurity program management Support
- Ensure cybersecurity documentation is accurate, current, and relevant to DOC
- Develop and provide training and outreach regarding security to DOC employees
- Effectively manage agency risk by maintaining visibility across the department

- Maintain comprehensive situational awareness of the cyber threat landscape as it relates to the DOC bureaus in support of the Department
- Reduce cost and optimize agency cybersecurity posture through complexity reduction and automation
- Deliver measurable cybersecurity outcomes
- Define and/or improve DOC's Cybersecurity Services Framework
- Effectively communicate with all parties, especially key stakeholders
- Improve Regulatory and Policy Alignment
- Improve cybersecurity program business processes

3.0 Requirement

3.1 Quality Assurance Surveillance Plan (QASP)

The Contractor shall monitor performance in accordance with the approved Quality Assurance Surveillance Plan (QASP). The Contractor shall develop and implement procedures to identify, prevent, and ensure non-recurrence of defective services in a Quality Control Plan (QCP). The Contractor's QCP is the means by which they will ensure work complies with the requirements of the BPA.

3.2 Workforce

The Contractor shall at all times maintain an adequate workforce for the uninterrupted performance of all tasks defined within this PWS when the Government facility is not closed. When hiring personnel, the Contractor shall consider the stability and continuity of the workforce are essential.

3.3 Clearance Requirements

Contractor employees must have a Top Secret/SCI security clearance prior to the start of the contract period of performance. The Department of Defense (DOD) 5220.22M National Industrial Security Program Operating Manual (NISPOM). DD form 254 applies to the base contract, and optional years.

Classified information, data, and/or equipment are not authorized for removal from DOC facilities.

3.4 Task Areas

The following task areas provide the required project, effort, or outcome expected:

3.4.1 Task Area 1: Program, Project, and Task Management

The Contractor shall name a program manager (PM) to serve as the Government's single focal point. The PM shall have responsibility for the planning, execution, control, and direction of prime contractor employees' and any subcontractors' programmatic and technical work performed under this BPA. The Contractor shall effectively and efficiently manage scope, quality, schedule, budget, resources, and risk using integrated program management processes across all aspects of performance and in a manner that yields cost savings and/or performance efficiencies.

The PM shall assure that the necessary controls for work described herein are appropriately supplied using program plans, program oversight, and reporting. The PM shall have the necessary authority to utilize the company's resources to assure the work under this BPA is accomplished

consistent with technical, cost, and schedule requirements as well as prudent programmatic and technical risk mitigation. The PM is responsible for designing and implementation of plans of action to ensure control and direction of contractor personnel is performed by management personnel of the Contractor, rather than the Government, and thus avoiding the delivery of personal services.

The Contractor shall provide cybersecurity program management, project management, task management, reporting, risk management, and issue management to ensure the success of programs, projects, and tasks in alignment with DOC's overall cybersecurity program goals.

The Contractor's program practices shall stress continuous and open communication with DOC, DOC's partnering contractors, and other stakeholders. Coordination and communication between the Contractor and DOC shall be conducted on both a formal and informal basis. Formal and informal liaison and coordination activities at the program level shall have performance issues as their main focus. Day-to-day interaction is typically required. Communications shall be conducted by telephone, email, reports, memoranda, and face-to-face interactions as necessary to conduct business in an efficient and effective manner.

The PM, and where needed other appropriate contractor personnel, shall participate in routine and periodic status meetings with key government personnel, at times on short notice. The purpose of such meetings is to ensure DOC stakeholders are informed of program status and progress on activities. The meetings provide an opportunity to set priorities, identify opportunities or concerns, and coordinate resolution of identified problems.

Utilizing an industry standard framework and methodology, the Contractor shall perform all program management functions. These functions, include but are not limited to, technical, business, risk and issue management functions that are necessary to execute the total effort required by this BPA. The Contractor shall provide all personnel and other resources, except as otherwise specified in this BPA, necessary to accomplish these functions. The Contractor shall affect these management functions through an integrated management approach, including cost, schedule, and technical performance. Consistent and meaningful communication between the Contractor and DOC is paramount at all levels from management down to government staff.

Assumptions:
DOC expects that all program managers or project managers will have extensive project management experience of 7 or more years managing programs or projects of comparable size, scope, and complexity to those described herein. The PM must possess an active Project Management Professional (PMP) certification from the Project Management Institute (PMI) at the time of contract award. See also BPA Labor Category descriptions.

3.4.2 Task Area 2: Program Support for Cybersecurity Programs

The Contractor shall provide program support services, including, but not limited to, the following:

a. Provide gap analyses, with recommendations for improvement, for the existing cybersecurity program.

b. Determine the impact of new tools, technologies, policies, mandates, or approaches (e.g., OMB mandates, CDM technologies, anomaly based tools, virtual environments, etc.) on the DOC cybersecurity program
c. Prepare meeting agenda, schedule meetings, capture meeting minutes and action items, obtain approval of meeting minutes, and publish approved meeting minutes and action items.
d. Provide expert analysis and document preparation for various analytical efforts focused on processes and procedures
e. Review various draft documents and provide timely feedback to DOC employees, customers, and contractors
f. Develop and implement cybersecurity and program strategic and tactical goals and objectives
g. Develop and implement cybersecurity and program outreach and communication plans
h. Identify and develop a Performance Management program that includes performance measures, tracking metrics, and trend analysis
i. Generate regular and ad hoc dashboards, reports, and metrics
j. Recommend, develop, and maintain monthly, quarterly, and annual FISMA reporting documents in DOC's required format
k. Attend working group meetings for OCRM working groups
l. Support and prepare internal and external response letters for submission such as FISMA transmittal, etc.
m. Using DOC provided management tools, maintain a DOC FISMA Risk Management report, that includes inventory, ATO and Plan of Action & Milestone (POA&M)s status, etc.
n. Using DOC provided management tools, maintain a tracking system of all OCRM cybersecurity-related deliverables— regularly scheduled and ad hoc
o. Provide DOC FISMA reporting tool administration
p. Assist the OCRM with transforming the cybersecurity organization and governance structure to support ongoing DOC initiatives
q. Prepare responses to federal ad hoc reporting requirements, to include, but not limited to, quarterly and annual FISMA Reports
r. Report on FISMA Inventory and provide POA&M reports monthly
s. Maintain project management documentation to support scope, schedule and budget of specific cybersecurity projects
t. Provide written recommendations for aligning the Boundary Protection effort with emerging Federal or industry cybersecurity priorities
u. Evaluate areas for performance or process improvement including analysis and reporting automation relevant cybersecurity priorities
v. Develop, support, consolidate, and analyze data call information collected from bureaus/operating units, as required.
w. Assist in coordination of responses from bureaus to support outside agencies requirements or requested information.
x. Provide architectural and technical guidance on enterprise-wide cybersecurity programs
y. Provide support for compliance with Office of Management and Budget (OMB), Congressional and other cybersecurity requirements and directives.

z. Provide support for IT Portfolio Management, including IT Portfolio Management implementation, application and investment analysis and budget and IT procurement support
aa. Publish information to DOC collaboration site(s) as required
bb. Develop and maintain program, project, and working group charters
cc. Prepare and publish monthly status reports
dd. Conduct capability maturity assessments
ee. Gather requirements for inter-agency agreements, memoranda of understanding, memoranda of agreement, and statements of work
ff. Track financial commitments, obligations, expenditures, and undelivered orders

3.4.3 Task Area 3: Information Security Subject Matter Expertise and Technical Advisory Services

3.4.3.1 Sub-Task 3.1: Cyber Security Policy and Documentation

The DOC Commerce Connection website provides agency employees and contractors a virtual library of applicable security policies, procedures, guidelines, tools, directives, and templates.

The Contractor, with OCRM direction, shall proactively review, update, and maintain cybersecurity policy, guidance documents, directives, templates, and materials to ensure all documentation reflects and incorporates the most recent version of all DOC cybersecurity program documentation.

The Contractor, with OCRM direction, shall provide Cyber security and Privacy requirements and guidance, including, but not limited to the following:

a. Provide a gap analysis, with recommendations for improvement, of existing Cyber security policies, handbooks, standards and procedures and recommend disposition (i.e. continued use as is, needs revision, or rescind)
b. Recommend, review and update existing, and/or develop new Cyber security policies, handbooks, standards, and procedures.
    i. Ensure documentation is current and relevant for DOC processes and programs
    ii. Ensure alignment with of security policy with agency programs like privacy, supply chain risk management, enterprise architecture, FISMA, etc.
c. Draft, review, and/or comment on CIO and CISO directives and other policies, procedures, and correspondence
d. Produce documentation, which includes security documentation, user manuals, training material, standard operating procedures (SOP), network diagrams, system-level security requirements, security specifications, and metrics for product/system testing evaluation and assessment.
e. Perform inventory review and update plan with schedule monthly
f. Delivery of Authority To Operate (ATO) packages review packages to CISO and CIO as required.

Assumptions:

1. The Contractor shall receive approval from DOC before any documents are made public or sent through the approval process for posting on the DOC Commerce Connection website.

2. The Contractor shall make sure any documents or updates to documents have gone through a quality control check for accuracy and appearance, including correction of spelling, grammar, and formatting errors, before submission to DOC.
3. The Contractor and OCRM shall agree on a timeframe for preparing, reviewing, and approving documents or updates to documents. This timeframe will be determined by the size, complexity, and breadth of the assignment.

3.4.3.2 Sub-Task 3.2: Supply Chain Risk Management (SCRM) Subject Matter Expert Services

DOC requires that the Contractor shall possess expertise in specific security or security-related supply chain topics, as necessary.

a. The Contractor shall provide overall subject matter expertise to the Supply Chain Risk Management. Provide specific guidance and technical expertise in the form of standards, policies, procedures, and oversight for the DOC SCRM program
b. Collect program information from the DOC enterprise and provide reports to the SCRM Program Manager (PM) and others as requested
c. Prepare reports on Enterprise SCRM for governing bodies
d. Recommend, develop, and maintain quarterly supply chain Congressional and other governing body reporting documents in DOC's required format.
e. Conduct initial IT SCRA acquisition package reviews for supply chain risk assessment packages submitted by customers.
f. Maintain the established tracking system documenting the number of assessments required and the status/disposition of supply chain risk assessment requests.
g. Prepare presentations and reports for SCRM PM regarding status of SCRM implementation, SCRA packages completed and in the SCRA investigators queue.
h. Provide recommendations to the SCRM Program manager regarding the need for more detailed review of individual requests.
i. Determine the impact of new or changing applicable federal policy changes
j. Determine the impact of new or revised legislation and regulations (OMB, FISMA, etc.)
k. Prepare situational awareness briefings regarding information security policy and contractor and developer trends for DOC senior management
l. Develop, update or improve the life cycle of the supply chain risk assessments including (but not limited to): supply chain risk assessment procedures, the SCRA, mitigation recommendations, compliance monitoring, continuous monitoring and reporting of IT vulnerabilities related to the supply chain.
m. Conduct research and present analyses to evaluate and/or determine risks to the supply chain:
    I. Contractor deliverables shall be in the form of white papers or development of PowerPoint briefing documentation as appropriate to the scope of the research, required analysis, and DOC method of dissemination and distribution.
    II. The Contractor may be required to provide strategic thought leadership and verbal briefings related to supply chain risk identification and mitigation and emerging industry issues and best practices.
    III. The Contractor shall be required to deliver written guidance or assessments in the form of short briefings, written documents, or presentations.

Assumptions:

1. The SCRM SME shall have an active Top Secret clearance and must be eligible to obtain access to DOC Sensitive Compartmented Information.
2. The SCRM SME shall have 5 years or more experience in supply chain risk management. The SME should have working knowledge of the NIST 800 Series. Individual also must have experience working with the NIST 800 Series, Committee on National Security Systems Directives for Supply Chain, and possess a working knowledge of risk management, and associated artifacts required by FISMA.
3. The SCRM SME shall receive approval from DOC before any documents are made public or sent through the approval process for posting on the DOC Commerce Connection website.
4. The SCRM SME shall ensure that any documents or updates to documents undergo a quality control check for spelling, grammar, and formatting errors before submission to DOC.
5. OCRM shall determine a reasonable timeframe for preparing, reviewing, and approving documents or updates to documents. This timeframe will be determined by the size, complexity, and breadth of the assignment.

3.4.3.3 Sub-Task 3.3 Continuous Diagnostics and Mitigation (CDM)

The Contractor shall provide support in the following areas including, but not limited to:

a. Technical support for current and future CDM phases to include technical knowledge of network and relay architecture, data flows, data aggregation, hardware and software asset management, secure configuration management, and vulnerability management, credential management, and privileged access management;
b. Maintenance of performance metrics related to the implementation of CDM;
c. Maintenance of executive management dashboards/reports on the Department's CDM program and all its phases;
d. Management and coordination of CDM implementation across DOC bureaus;
e. Assistance with working group meetings including maintenance of minutes and tracking action items;
f. Project management support related to implementation of current and future CDM phases across DOC and its bureaus;
g. Engagement and communication with key stakeholders in CDM and ICAM efforts.

3.4.3.4 (Ad Hoc) Sub Task 3.4: Ad-hoc Security Engineering Subject Matter Expert Services

The Contractor shall possess expertise in specific security or security-related engineering topics, as necessary. The Contractor Security Engineering SME expertise shall include, but is not limited to, the following types of ad hoc activities, which could occur several times a month:

a. Prepare situational awareness briefings regarding information security policy and contractor and developer trends for DOC senior management
b. Develop alternatives of system designs and/or architectures which consider trade-offs between security requirements, functional/operational requirements and cost.
c. Review and describe the impact of new or changing federal policies
d. Review and describe the impact of new or revised legislation and regulations (OMB, FISMA, etc.)

e. Provide security engineering subject matter expertise in coordination with Enterprise Architecture and Technical Review Board to conduct technical review board program planning reviews related to future enterprise architecture updates and proposed information security mechanisms
    i. Support will be technology-related architecture guidance delivered in the form of PowerPoint briefings, email, or white papers addressing information security architecture vulnerabilities, risks, mitigation response, and emerging opportunities
f. Conduct research and present analyses to evaluate and/or identify and describe emerging industry technology trends, government agency best practices, and security issues:
    i. Contractor deliverables shall be in the form of white papers or development of PowerPoint briefing documentation as appropriate to the scope of the research, required analysis, and DOC method of dissemination and distribution.
    ii. The Contractor may be required to provide strategic thought leadership and verbal briefings related to security engineering risk identification and mitigation and emerging industry issues and best practices.
    iii. The Contractor shall be required to deliver written guidance or assessments in the form of short briefings, written documents, or presentations.

Assumptions:

1. The Contractor shall ensure that any documents or updates to documents undergo a quality control check for spelling, grammar, and formatting errors before submission to DOC.
2. OCRM shall determine a reasonable timeframe for preparing, reviewing, and approving documents or updates to documents. This timeframe will be determined by the size, complexity, and breadth of the assignment.

3.4.4 Task Area 4: Assessment Services

3.4.4.1 (Ad Hoc) Sub Task 4.1: Security Assessment and Authorization (A&A) Subject Matter Expert Support

a. The Contractor shall provide overall subject matter expertise to the Information Security Assessment and Authorization (A&A) program that currently comprises over 250 FISMA systems of varying size and complexity. Provide specific guidance and technical expertise in the form of standards, policies, procedures, and oversight for the DOC A&A program
b. Review and provide recommendations based on analysis for Privacy Impact Assessments (PIA)
c. Review and provide recommendations based on analysis for Third Party Website and Applications (TPWA)
d. Review and analyze all system artifacts for accuracy, completeness, in support of an authorization to operate (ATO) requests
e. Create or Review ATO packages prior to submission to CISO and CIO approval
f. Ensure all assessment and audit reports are uploaded properly to the DOC FISMA tool
g. Conduct reviews of closed Plan of Actions and Milestones (POA&M) for completeness and compliance
h. Develop and support the ongoing authorization (OA) process that includes continuous monitoring

i. Draft document, review and provide feedback on application of security requirements (e.g. TRB, review of SSPs, RA's, contingency plan, POA&M reports).

j. Perform Assessments and Analysis (A&A) on a firm fixed price basis for NEW and RECERT (i.e., re-authorizations) Authorizations to Operate (ATO) for the three levels of systems defined below. The security controls to be assessed are contained in NIST 800-53, with the current publication (rev 4) accessible at https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final). The potential duration is for reference purposes only and fixed prices associated with A&As for the various system levels is not subject to change based on actual duration.

System Level	# of Controls to be Assessed	Potential Duration
1 (Low)	166	2 to 3 months
2 (Moderate)	303	More than 3 but less than 4 months
3 (High)	385	4 months or greater

Assumptions:

1. The A&A SME shall have an active Top Secret clearance and must be eligible to obtain access to DOC Sensitive Compartmented Information.
2. The A&A SME shall have 5 years or more experience actively working with the NIST 800 Series, and hold at least one professional security certification related to subject. Individual also must have experience working with FIPS 200, FISMA, the Privacy Act, and possess a working knowledge of risk management, and associated artifacts required by FISMA.

3.4.4.2 (Ad Hoc) Sub Task 4.2: Supply Chain Risk Assessment Services

DOC IT systems require Supply Chain Risk Assessment (SCRA) Services which shall be provided by the Contractor. The SCRA services may include, but is not limited to, the following types of ad hoc activities, which could occur several times a month:

a. Support supply chain risk assessment (SCRA) research to include (but not limited to): publicly available and all-source intelligence.
b. Conduct research and present analyses to evaluate and/or determine risks to the supply chain:
   I. Contractor deliverables shall be in the form of supply chain risk assessments and development of PowerPoint briefing documentation as appropriate to the scope of the research, required analysis, and DOC method of dissemination and distribution.
   II. The Contractor may be required to provide strategic thought leadership and verbal briefings related to supply chain risk identification and mitigation and emerging industry issues and best practices.
c. The Contractor shall be required to deliver written guidance or assessments in the form of short briefings, written documents, or presentations.
d. Develop, update or improve the life cycle of the supply chain risk assessments including (but not limited to): supply chain risk assessment procedures, the SCRA, mitigation recommendations, compliance monitoring, continuous monitoring and reporting of IT vulnerabilities related to the supply chain.

e. Perform Supply Chain Risk Assessments (SCRAs) on a firm fixed price basis across the three Levels of SCRAs as described below.

SCRA Level	# of Supply Chain Hops	# of Original Equipment Manufacturers (OEMs)	# of Value Added Resellers (VARs)	# of Unique Products for Analysis
1	3 or fewer	2 or fewer	2 or fewer	50 or fewer
2	4 to 5	3 to 4	3	51 to 100
3	Over 6	Over 4	Over 3	Over 100

SCRA complexity grows from a Level 1 up to Level 3 based upon the number of Supply Chain Hops, OEMs, VARs and Unique Products being analyzed. Additional complexity factors may include foreign ownership deemed "high-risk". The table above will be used as a general guideline on SCRA complexity while also considering other important factors that may affect complexity and required level of effort.

Assumptions:

1. The Contractor shall possess an active Top Secret clearance and must be eligible to obtain access to DOC Sensitive Compartmented Information.
2. The Contractor shall receive approval from DOC before any documents are made public or sent through the approval process for posting on the DOC Commerce Connection website.
3. The Contractor shall ensure that any documents or updates to documents undergo a quality control check for spelling, grammar, and formatting errors before submission to DOC.
4. OCRM shall determine a reasonable timeframe for preparing, reviewing, and approving documents or updates to documents. This timeframe will be determined by the size, complexity, and breadth of the assignment.

3.4.4.3 (Ad Hoc) Sub Task 4.3 Third Party/Interconnection Security and FedRAMP

The Contractor shall support security assessment requirements in support of third party and the risk associated with interconnections; as specified under FISMA. The contractor shall:

a. Develop and review plans to assess the security controls.
b. Assess security controls in accordance with the assessment procedures defined in the security assessment plan.
c. Prepare security assessment reports that document the issues, findings, and recommendations based on the security control assessment.

3.4.5 Task Area 5: Cyber Security Awareness Training

The Contractor shall provide subject matter expert support for the development, delivery and maintenance of a comprehensive cybersecurity awareness and training program. This program will include, but is not limited to, providing support in the following areas:

a. Provide a gap analysis, with recommendations for improvement, of the existing training program and materials.
b. Develop, deliver and maintain outreach and marketing strategy for cybersecurity.
c. Engage with the CISO and Information Technology Security Officer (ITSO) community to communicate changes to DOC programs

d. Enhance, document, administer, and deliver a comprehensive program to measure and improve the cybersecurity awareness and vigilance of DOC system users, including those with significant security responsibilities
e. Develop and implement reporting and tracking processes for information security awareness and role-based information security training
f. Provide information security training (classroom, web-based, and other methods) across the gamut of information security, including DOC cybersecurity specific topics and recent industry trends
g. Provide support to the development, implementation, and tracking of role-based information security training
h. Troubleshoot and provide solutions to issues with information security training software
i. Provide support to the coordination of training seminars, training meetings, conferences, etc.

Material developed for training may be in the form of, but are not limited to, audio, visual, computer-based, Web-based, or written media as directed by DOC. The Contractor may be required to provide instructors to present any of the material developed in the form of (but not limited to) classroom instruction, small group discussions, briefings, etc., as directed by DOC. The ability to allow courses to be captured electronically for use by personnel who cannot attend the training in person should be available. In addition, the Contractor shall develop and provide courses in other formats, including (but not limited to) webinars, avatar, PowerPoint presentations, etc. DOC will determine the distribution of the type of training to be provided with input from the Contractor.

The Contractor shall develop the following material for each class:

a. For classroom training:
   i. Student handout that contains a copy of the course briefing and/or other supporting material
   ii. A copy of the course briefing and/or other supporting material archived to DOC training folder

b. For all courses:
   i. Course evaluation to be completed by each individual attending the class.
   ii. Certificate of Attendance to be awarded to each individual completing the class.
   i. Proficiency examination that will be administered by the Contractor at the conclusion of each class, if warranted by the content.
   ii. Certificate of Accomplishment for individuals successfully completing the examination. If appropriate, this certificate may be in the form of a Committee for National Security Systems (CNSS) or other Government-recognized certification.
   iii. Electronic copy (e.g., Acrobat file) of the scanned image of the completed course evaluations
   iv. Attendance file for upload to DOC Computer Based Training System (CBT) to record attendance.
   v. Trainings are made Section 508 compliant.
   vi. Course curriculum

In addition to training, the Contractor shall develop and execute an outreach and marketing campaign to include a strategy. Once the government approves the strategy, the Contractor shall

execute the strategy. Additionally, the Contractor shall develop all materials to include brochures and slick sheets. The Contractor shall also conduct outreach activities such as brown bags and displays.

Assumptions:

1. Classroom training and outreach will be conducted at the DOC HQ location. Attendees could be remote.
2. The Government shall provide the room/space for all meetings.
3. Training shall be all-encompassing (including the cost of all course material and assembly).
4. The Contractor shall make sure any documents or updates to documents have gone through a quality control check for spelling, grammar, and formatting errors before submission to DOC.
5. On average during the calendar year the Contractor conducted 2 - 3 in person classes per month and 2 remote classes per month. Examples include: Cybersecurity Essentials, Risk Management, Contingency Planning and Assessment & Authorization.
6. The Contractor shall conduct brown bag seminars on various cybersecurity topics on a monthly basis
7. Training team must maintain an average feedback rating at or above 8.5 out of 10 on Course Evaluation forms.
8. Trainer must have at least 5-years' experience developing and providing training.

3.4.6 Task Area 6: Audit Management

DOC requires the Contractor to provide subject matter expertise and audit management support for involvement in the development and maintenance of an Audit and Risk Management program. OCRM facilitates audits for various reason to include requests from The Government Accountability Office, FISMA compliance, Office of Management and Budget Circular A-123 Management's Responsibility for Internal Controls, and Audits, Chief Financial Officer (CFO) audits, and Office of Inspector General (OIG) audits.
The Contractor will provide support to include, but not limited to, providing support in the following areas:

a. Gap analysis and recommendations for improvement of the current audit management program
b. Gap analysis and recommendation on current corrective and audit action plans
c. Maintain audit requests and responses in a manner that is accessible by multiple stakeholders
d. Support the Audit Liaison in research, gathering, and submission of audit-related artifacts
e. Support the Audit Liaison in research and writing audit responses
f. Maintain a tracking process that follows the findings through remediation and closure
g. Manage each audit engagement in collaboration with all stakeholders
h. Assist with creating finding spreadsheets based upon audit reports, for upload to the designated tool set
i. Assist with managing and maintaining visibility of plans of action and milestones (POA&M) to achieve acceptable levels of risk
j. Maintenance of metrics to show progress of audit work
k. Report on audit and risks as required,
l. Meet due dates and deadlines for audit work and responsibilities.

Assumptions

1. The contractor shall have at least 2 years of experience with an IT audit support program.
2. The Contractor and OCRM shall agree on a timeframe for preparing, reviewing, and approving documents or updates to documents. This timeframe will be determined by the size, complexity, and breadth of the assignment.
3. The Contractor shall obtain government approval prior to contacting any stakeholders external to OCRM for data collection or other information.
4. The Contractor must provide draft documents as agreed upon by the PM and COR; the final report shall be due 5 days after receiving government input on a draft report.

4.0 Place of Performance

Contractor support shall perform at DOC Herbert C. Hoover Building, Washington, DC.

☒ Remote/telework may be authorized by the Task Manager (TM) on a case by case basis.

5.0 Period of Performance

The total period of performance with all options exercised is for 5 years from date of award.

Base Period:	June 11, 2018 through June 10, 2019
Option Period I:	June 11, 2019 through June 10, 2020
Option Period II:	June 11, 2020 through June 10, 2021
Option Period III:	June 11, 2021 through June 10, 2022
Option Period IV:	June 11, 2022 through June 10, 2023

6.0 Hours of Operation

Under this BPA, the Contractor is responsible for conducting business, Monday through Friday during normal business hours of 7:00 a.m. to 6:00 pm except Federal holidays or when the Government facility is closed due to local or national emergencies, administrative closings, or similar Government directed facility closings.

7.0 Government Furnished Resources

7.1 The Contractor shall be responsible for safeguarding all government equipment, information and property provided for Contractor use. The Contractor shall not use GFP/E/I for any purposes other than official Government business as performed under this BPA. At the close of each work period, government facilities, equipment, and materials shall be secured.

7.2 Contractor personnel working on Government sites will be provided standard business equipment including all or some of the following: desk, chair, phone, computer and access to office equipment such as printers, copiers, fax, etc. as appropriate.

8.0 Qualifications

The Contractor shall be responsible for and shall ensure staff are properly trained and hold the appropriate credentials as required and/or necessary for the services being performed.

9.0 Key Personnel

All proposed substitutions of key personnel shall be submitted, in writing, to DOC at least thirty (30) days prior to the proposed substitution, or as soon as reasonably known, whichever is earlier.

Each request shall provide a detailed explanation of the circumstances necessitating the proposed substitution, a complete resume, and any other information required by DOC. All proposed substitutions shall have qualifications equal to or greater than the person(s) being replaced.

10.0 Identification of Contract Employees

All Contractor personnel attending meetings, answering Government telephones, and working in other situations where their Contractor status is not obvious to third parties are required to identify themselves as such to avoid creating an impression in the minds of members of the public that they are Government officials. They must also ensure that all documents or reports produced by Contractors are suitably marked as Contractor products or that Contractor participation is appropriately disclosed.

11.0 Travel

Travel ☒ is ☐ is not required under this BPA.

If required, the Contractor shall travel as approved by the designated TM or COR during the performance of this BPA to attend meetings, conferences or conduct other official business covered under this BPA. Authorized travel is reimbursable in accordance with the contract. The Contractor shall ensure adequate funding is available for costs of travel prior to incurring costs.

Local travel to meetings, conferences or other official business covered under this BPA is not reimbursable as a direct charge.

12.0 Conflict of Interest

Contractor and subcontract personnel performing work under this BPA may receive, have access to, or participate in the development of proprietary or source selection information (e.g., cost or pricing information, budget information or analyses, specifications or work statements, etc.), or perform evaluation services which may create a current or subsequent Organizational Conflict of Interests (OCI) as defined in FAR Subpart 9.5. The Contractor shall notify the CO immediately whenever he/she becomes aware that such access or participation may result in any actual or potential OCI, and may merit the submittal of a plan to the CO to avoid or mitigate any such OCI. This mitigation plan shall be determined to be acceptable solely at the discretion of the CO. In the event the CO unilaterally determines that any such OCI cannot be satisfactorily avoided or mitigated, the Contracting Officer may employ other remedies as he or she deems necessary, including prohibiting the Contractor from participation in subsequent contracted requirements which may be affected by the OCI. DOC reserves the right to take any and all responsive measures (including Contractor termination) available under applicable laws and regulations.

13.0 Data Rights

The Government has unlimited rights to all documents/material produced under this BPA. All documents and materials, to include the source code of any software produced under this contract, shall be Government owned and the property of the Government with all rights and privileges of ownership/copyright belonging exclusively to the Government. These documents and materials may not be used or sold by the Contractor without written permission from the CO. All

materials supplied to the Government shall be the sole property of the Government and may not be used for any other purpose. This right does not abrogate any other Government rights.

14.0 Applicable Publications (Current Editions)

☐ No publications are applicable for this award.
☒ The following list of publications is applicable to this BPA:

- Executive Order 12829, *"National Industrial Security Program,"* January 6, 1993.
- Executive Order 13526, *Classified National Security Information*, December 29, 2009.
- DoD 5220.22-M, change 2, *National Industrial Security Program Operating Manual,* March 28, 2013.
- *National Industrial Security Program Manual, Change 2*, May 18, 2016
- CNSSI-1253, *Security Categorization and Control Selection for National Security Systems*, March 27, 2014.
- CNSSI-4009, *Committee on National Security Systems (CNSS) Glossary*, April 6, 2015
- CNSSI-7003, *Protected Distribution Systems (PDS),* September 30, 2015.
- NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*, February 2010. (updated June 5, 2014).
- NIST SP 800-53, Revision 4, *Recommended Security Controls for Federal Information Systems and Organizations*, April 2013 (Updates as of January 22, 2015).
- NIST SP 800-53A, Revision 4, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans* December 2014.
- NIST SP 800-60, Volume 1, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories,* Aug 2008.
- NIST SP 800-61, Revision 2, *Computer Security Incident Handling Guide*, August 2012.
- NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations* September 2011.
- NIST SP 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations* April 2015.
- FIPS 140-2, *Security Requirements for Cryptographic Modules*, May 25, 2001; Change notice December 3, 2002.
- CNSSD 504, *Directive on Protecting National Security Systems from Insider Threat*
- CNSSD 505, *Supply Chain Risk Management.*
- Executive Order 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing of Classified Information.*
- Presidential Memorandum, *National Insider Threat Policy and Minimum Standards for Executive Branch Threat Programs.*

15.0 Reports and Deliverables

15.1 The Contractor shall attend progress meetings requested by the contracting activity or BPA/task order administration officials. The Contracting Officer, Contracting Officer's Representative (COR), and other Government personnel, as appropriate, may meet periodically with the Contractor to review the Contractor's performance. At these meetings the CO will apprise the Contractor of how the government views the Contractor's

performance and the Contractor will apprise the Government of problems, if any, being experienced. Appropriate action shall be taken to resolve outstanding issues. These meetings shall be at no additional cost to the government.

15.2 The Contractor shall prepare and submit a monthly progress report describing at a minimum the work performed during the month, the projected work over the next month, and any issues or barriers that need to be addressed.

16.0 Attachment/Technical Exhibit List

16.1 Attachment 1/Technical Exhibit 1 - Performance Requirements Summary

16.2 Attachment 2/Technical Exhibit 2 – Deliverables Schedule

TECHNICAL EXHIBIT 1

Performance Requirements Summary

The Contractor service requirements are summarized into performance objectives that relate directly to mission essential items. The performance threshold briefly describes the minimum acceptable levels of service required for each requirement. These thresholds are critical to mission success.

Performance Objective (The Service required—usually a shall statement)	***Performance Standard***	**Performance Threshold** (This is the maximum error rate. It could possibly be "Zero deviation from standard")	**Method of Surveillance**
PRS # 1. The Contractor shall provide program management support PWS paragraph (3.4.1)	The Contractor provided 30 days after award.	*95% compliance*	*Review of report*
PRS #2 Monthly Financial and Status Reports (3.4.1)	10th business day of the month	*95% Compliance*	*Review of monthly reports/random monitoring*
PRS #3 The Contractor shall provide Cyber Security Program Gap Analysis and Recommendations (3.4.2)	30 days after contract award or as negotiated with the Government	*100% inspection of finished product*	*Review of Gap Analysis and Recommendations*
PRS #4 The Contractor shall provide updated cybersecurity and program strategic and tactical plans (3.4.2)	30 days after contract award or as negotiated with the Government	*100% inspection of finished product*	*Review of Plan*
PRS #5 The Contractor shall provide FISMA reports (3.4.2)	15 days prior to due date or as negotiated with the Government	*100% inspection of finished product*	*Review of Reports*
PRS #6 The Contractor shall provide Cyber Security Situational Awareness Briefings (3.4.2)	Within 5 days of established due date	*100% inspection of finished product*	*Review of Briefing*

PRS #7 The Contractor shall provide Cyber Security Policy Gap Analysis and Recommendations (3.4.3.1)	45 days after contract award or as negotiated with the Government	*100% inspection of finished product*	*Review of Gap Analysis and Recommendations*
PRS #8 The Contractor shall provide Quarterly Congressional Reporting (3.4.3.2)	15 days prior to the end of the quarter	*100% inspection of finished product*	*Review of materials*
PRS #9 The Contractor shall develop an ongoing authorization (OA) plan (3.4.4.1)	Within 60 days of contract award	*100% inspection of finished product*	*Review of Plan*
PRS #10 The Contractor shall create ATO packages (3.4.4.1)	Within 15 days of ATO expiration	*100% inspection of finished product*	*Review of Packages*
PRS #11 The Contractor shall develop analysis of application of security requirements (e.g. TRB, review of SSPs, RA's, contingency plan, POA&M reports). (3.4.4.1)	Within 5 days of established due date	*100% inspection of finished product*	*Review of Report*
PRS #12 The Contractor shall provide Supply Chain Risk Assessments Communication (3.4.4.2)	Bi-weekly update or as negotiated with Government.	*No more than one customer complaint per engagement.*	*Validated Customer Complaint received by COR.*
PRS # 13 The Contractor shall provide Supply Chain Risk Assessments Reports (3.4.4.2)	Within 7 business days of request or as negotiated with Government.	*100% inspection of finished product*	*Review of Reports*

PRS #14 The Contractor shall provide gap analysis and recommendations for the Cyber Security Training program (3.4.5)	30 days after contract award; one time deliverable	*100% inspection of finished product*	*Review of Gap Analysis and Recommendations*
PRS #15 The Contractor shall provide Cyber Security Outreach and Marketing Strategy (3.4.5)	30 days after contract award; one time deliverable	*100% inspection of finished product*	*Review of Strategy*
PRS #16 Cyber Security Training curriculum (3.4.5)	45 days after contract award; one time deliverable	*100% inspection of finished product*	*Review of curriculum*
PRS #17 The Contractor shall provide Cyber Security training course materials (3.4.5)	Within 15 days of established due date	*100% inspection of finished product*	*Review of materials*
PRS #18 The Contractor shall provide Gap analysis Audit corrective action plans (3.4.6)	45 days after contract award	*100% inspection of finished product*	*Review of plans*

TECHNICAL EXHIBIT 2

DELIVERABLES SCHEDULE

This technical exhibit lists any reports or documentation that is required as a deliverable to include the frequency, # of copies, medium/format and who/where it is to be submitted. A deliverable is anything that can be physically delivered but may include non-physical things such as meeting minutes. This deliverables schedule is representative of the type of schedule that may be included in task orders placed against this BPA.

Deliverable	Frequency	# of Copies	Medium/Format	Submit To
Monthly Progress Report (3.4.1)	Monthly by the 5th of each month covering the previous month.	1 copy submitted electronically by email	MS Office or PDF formats	TM, COR, CO
Monthly Financial and Status Reports (3.4.1)	10th business day of the month	1 copy submitted electronically by email	MS Office or PDF formats	TM, COR, CO
Cyber Security Situational Awareness Briefings (3.4.2)	Within 5 days of established due date	1 copy submitted electronically by email	MS Office and PDF formats	TM, COR
Publish required information to DOC collaboration site(s) (3.4.2)	As requested	1 copy submitted via publishing to DOC collaboration site	MS Office or PDF formats	TM, COR
Provide impact of new tools, technologies, policies, mandates, or approaches on the DOC cybersecurity program (3.4.2)	As requested	1 copy submitted via publishing to DOC collaboration site	MS Office or PDF formats	TM, COR
Prepare meeting agenda, schedule meetings, capture meeting minutes and action items,	As requested	1 copy submitted via publishing to DOC	MS Office or PDF formats	TM, COR

Deliverable	Frequency	# of Copies	Medium/Format	Submit To
obtain approval of meeting minutes, and publish approved meeting minutes and action items. (3.4.2)		collaboration site		
Provide timely feedback to DOC employees, customers, and contractors (3.4.2)	As requested	1 copy submitted via publishing to DOC collaboration site	Email, Phone, MS Office or PDF formats	TM, COR
Program outreach and communication plans (3.4.2)	As requested	1 copy submitted via publishing to DOC collaboration site	MS Office or PDF formats	TM, COR
Performance Management program (3.4.2)	Monthly	1 copy submitted via publishing to DOC collaboration site	MS Office or PDF formats	TM, COR
Dashboards, reports, and metrics (3.4.2)	Monthly and as requested	1 copy submitted via publishing to DOC collaboration site	MS Office or PDF formats	TM, COR
FISMA Risk Management report (3.4.2)	Monthly and as requested	1 copy submitted via publishing to DOC collaboration site	MS Office or PDF formats	TM, COR
Maintain a tracking system of all OCRM cybersecurity-related	Weekly and as requested	1 copy submitted via publishing to DOC collaboration site	MS Office or PDF formats	TM, COR

Deliverable	Frequency	# of Copies	Medium/Format	Submit To
deliverables (3.4.2)				
Recommendations for aligning the Boundary Protection (3.4.2)	Weekly and as requested	1 copy submitted via publishing to DOC collaboration site	MS Office or PDF formats	TM, COR
Data Calls. (3.4.2)	As requested	1 copy submitted via publishing to DOC collaboration site	MS Office or PDF formats	TM, COR
IT Portfolio Management (3.4.2)	Bi-weekly and as requested	1 copy submitted via publishing to DOC collaboration site	MS Office or PDF formats	TM, COR
Publish information to DOC collaboration site(s) as required (3.4.2)	As requested	1 copy submitted via publishing to DOC collaboration site	DOC collaboration site	TM, COR
Working group charters (3.4.2)	As requested	1 copy submitted via publishing to DOC collaboration site	MS Office or PDF formats	TM, COR
Prepare and publish status reports (3.4.2)	Monthly	1 copy submitted via publishing to DOC collaboration site	MS Office or PDF formats	TM, COR
Track financial commitments, obligations, expenditures, and	Weekly and as requested	1 copy submitted via publishing to DOC	MS Office or PDF formats	TM, COR

Deliverable	Frequency	# of Copies	Medium/Format	Submit To
undelivered orders (3.4.2)		collaboration site		
Cyber Security Program Gap Analysis and Recommendations (3.4.2)	30 days after contract award; one time deliverable	1 copy submitted electronically by email	MS Office or PDF formats	TM, COR
Update cybersecurity and program strategic and tactical plans (3.4.2)	30 days after contract award; one time deliverable	1 copy submitted electronically by email	MS Office or PDF formats	TM, COR
Quarterly and Annual FISMA reports (3.4.2)	15 days prior to established due date; quarterly and annual deliverable	Multiple copies submitted by email	MS Office or PDF formats	TM, COR
Cyber Security Policy Gap Analysis and Recommendations (3.4.2)	45 days after contract award; one time deliverable	1 copy submitted electronically by email	MS Office or PDF formats	TM, COR
Final policy (3.4.3.1)	30 days after completion of the policy; delivered on annual basis	1 copy submitted electronically by email	MS Office or PDF formats	TM, COR
Draft procedures (3.4.3.1)	In conjunction with policy development ; delivered on annual basis	1 copy submitted electronically by email	MS Office or PDF formats	TM, COR
Finalize procedures (3.4.3.1)	30 days after approval of Draft SCRA procedures one time deliverable	1 copy submitted electronically by email	MS Office or PDF formats	TM, COR
SCRM Reports on Enterprise Supply Chain Risk (3.4.3.2)	Quarterly 12 days before submission deadline (14th	1 copy submitted electronically by email	MS Office	TM, COR

Deliverable	Frequency	# of Copies	Medium/Format	Submit To
	of the 1st month of each quarter) and as requested			
Create ATO packages (3.4.4.1)	Within 15 days of ATO expiration	3 copies; paper and electronic by email	MS Office and PDF formats	TM, COR
Develop application of security requirements (e.g. document controls implementation, update and/or create a SSPs, RA's, contingency plan, POA&Ms, etc). (3.4.4.1)	Within 5 days of established due date	1 copy submitted electronically by email	MS Office and PDF formats	TM, COR
Create or maintain ATO packages (e.g. required documentation [SSP, RA, CP, Continuous monitoring plan, etc.], POA&M creation/update/ maintenance) (3.4.4.1)	Within 5 days of established due date	1 copy submitted electronically by email	MS Office and PDF formats	TM, COR
Develop analysis of application of security requirements (e.g. TRB, review of SSPs, RA's, contingency plan, POA&M reports). (3.4.4.1)	Within 5 days of established due date	1 copy submitted electronically by email	MS Office and PDF formats	TM, COR
Develop an ongoing authorization	Within 60 days of	1 copy submitted	MS Office and PDF formats	TM, COR

Deliverable	Frequency	# of Copies	Medium/Format	Submit To
(OA) plan (3.4.4.1)	contract award	electronically by email		
Cyber Security Situational Awareness Briefings (3.4.4.1 and 3.4.4.2)	Within 5 days of established due date	1 copy submitted electronically by email	MS Office and PDF formats	TM, COR
Final DOC Quarterly SCRM Review and PL113-235 515 Requirement OMB on Enterprise Supply Chain Risk (3.4.4.2)	Quarterly 2 days after approval of Draft report	1 copy submitted electronically by email	MS Office	TM, COR
Support reporting to GAO, OMB, Congress, and other governing bodies (3.4.4.2)	5 days upon Government request, unless additional time is documented and agreed upon	1 copy submitted electronically by email	MS Office or PDF formats	TM, COR
Conduct initial SCRA package completeness review (3.4.4.2)	1 day upon Government request, unless additional time is documented and agreed upon	1 copy submitted electronically by email	MS Office or PDF formats	TM, COR
Download SCRA request packages, prepare SCRA packages and submit SCRA packages to the SCRA	1 business day of SCRA request	1 copy submitted electronically by email	MS Office or PDF formats	TM, COR

Deliverable	Frequency	# of Copies	Medium/Format	Submit To
investigator. (3.4.4.2)				
Update an automated SCRA tracking system (3.4.4.2)	1 business day of SCRA request	1 copy submitted electronically by email	MS Office or PDF formats	TM, COR
Prepare SCRA package status up-date for customers. (3.4.4.2)	Bi-weekly	1 copy submitted electronically by email	MS Office or PDF formats	TM, COR
Up-to-date working group point-of-contact lists (3.4.4.2)	Monthly	1 copy submitted electronically by email	MS Office or PDF formats	TM, COR
Up-to-date working group mailing lists (3.4.4.2)	Monthly	1 copy submitted electronically by email	MS Office or PDF formats	TM, COR
Meeting minutes (3.4.4.2)	Three business days after meeting conclusion	1 copy submitted electronically by email	MS Office or PDF formats	TM, COR
Meeting invitations sent out electronically (3.4.3.3)	Three business days prior to scheduled meeting dates	1 copy submitted electronically by email	MS Office or PDF formats	TM, COR
Develop reports that include statistical information regarding program accomplishments (3.4.3.3)	Monthly	1 copy submitted electronically by email	MS Office or PDF formats	TM, COR
Develop risk threshold determinations (3.4.3.3)	7 business days after request and	1 copy submitted electronically by email	MS Office or PDF formats	TM, COR

Deliverable	Frequency	# of Copies	Medium/Format	Submit To
	annually thereafter			
Support Supply Chain Risk Assessments (3.4.3.4)	14 days upon Government request, unless additional time is documented and agreed upon.	1 copy submitted electronically by email	MS Office or PDF formats	TM, COR
Create a detailed SCRA report for the assigned actions. The assessments should include risk analysis that documents the threat-vulnerability pairing that shall correspond to the most current revision of NIST SP 800 series and CNSS Directive 505. (3.4.3.4)	Within 2 days of research completion.	1 copy submitted electronically by email	MS Office or PDF formats	TM, COR
Provide unclassified or classified security briefing of assessment report. (3.4.3.4)	Within 5 days of request.	1 copy submitted electronically by email	Verbal	TM, COR
Develop training and awareness strategy (3.4.4)	90 days after contract award one time deliverable	1 copy submitted electronically by email	MS Office or PDF formats	TM, COR
Hold a stand-up event with a guest speaker (3.4.4)	120 days after contract award and	1 copy submitted electronically by email	MS Office or PDF formats	TM, COR

Deliverable	Frequency	# of Copies	Medium/Format	Submit To
	once quarterly thereafter			
Gap analysis and recommendations for the Cyber Security Training program (3.4.4)	30 days after contract award; one time deliverable	1 copy submitted electronically by email	MS Office or PDF formats	TM, COR
Cyber Security Outreach and Marketing Strategy (3.4.4)	30 days after contract award; one time deliverable	1 copy submitted electronically by email	MS Office or PDF formats	TM, COR
Cyber Security Training curriculum (3.4.4)	45 days after contract award; one time deliverable	1 copy submitted electronically by email	MS Office or PDF formats	TM, COR
Cyber Security training course materials (3.4.4)	Within 15 days of established due date	Delivered electronically and on paper	MS Office or PDF formats	TM, COR
Gap analysis Audit corrective action plans (3.4.5)	45 days after contract award	1 copy submitted electronically by email	MS Office or PDF formats	TM, COR