NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY
7500 GEOINT Drive
Springfield, Virginia 22150

June 07, 2016

SUBJECT: Request for Information – Cybersecurity and Risk Management aka: Cybertron

The National Geospatial Intelligence Agency is issuing a Request for Information for the Cybertron contract for public review and comment. The requirements for Cybertron currently exist under the NGA Enterprise Support to Management And Resources for Technical Services (ESMARTS) contract, but will not be competed with the MOHAVE contract.

The RFI is issued in accordance with FAR 52.215-3, Request for Information or Solicitation for Planning Purposes (Oct 1997), with the purpose of assisting the Government in developing the highest quality Performance Work Statement (PWS) and solicitation possible. Accordingly, industry is requested to respond to the questions provided in the RFI and comment on all aspects of the draft PWS.

Responses to this RFI must be submitted on or before July 07, 2016 at 1600 EST to be considered by the Government. Submissions should not contain proprietary markings and must be submitted in writing to CyberRiskMgmt@nga.mil. This RFI will be posted to various sites such as GSA e-Buy, Federal Business Opportunities (FBO), and various GWACs to ensure the widest dissemination possible.

The Government may not respond to comments, however, all comments received prior to the due date and time will be considered and, as appropriate, resulting revisions may be incorporated into a future solicitation.

This RFI is not a solicitation and NGA is not requesting proposals at this time. Therefore, it shall not be constructed as a commitment on the part of the Government to award a contract nor does it obligate the Government for costs incurred in the preparation and submittal of proposals in anticipation of a contract. Any subsequent requests for information or solicitations will be announced on the Federal Business Opportunities (FedBizOpps) website (www.fbo.gov). It is the responsibility of the prospective offerors to monitor the internet sites for any releases of information (if any).

Thank you for your interest and participation in this RFI.

Rose M. Schultz
Contracting Officer

REQUEST FOR INFORMATION
Cybersecurity and Risk Management

1.0 Description & Purpose

1.1 The National Geospatial-Intelligence Agency (NGA), in support of the Cybersecurity and Risk Management acquisition, is seeking information on how an interested contractor could assist NGA by sharing its comments on the information described within the attached Draft Performance Work Statement (PWS) and the areas described below.

1.1.1 The Draft PWS contains citations that are listed as To Be Determined (TBD). As part of their response, respondents are invited to submit comments/recommendations regarding the subject matter containing said citation.

1.2 The purpose of this Request for Information (RFI) is to gain information on current Industry practices that would meet NGA's requirements and to assess industry interest in participating in any subsequent acquisitions for these services.

1.3 **This is a Request for Information (RFI) only**. This RFI is issued solely for information and planning purposes. It does NOT constitute a Request for Proposal (RFP) or a promise to issue an RFP in the future. This request for information does not commit the Government to contract for any supply or service whatsoever. Further, NGA is not at this time seeking proposals and will not accept unsolicited proposals. Interested Parties who chose to responds are advised that the U.S. Government will not pay for any information or administrative costs associated with their response to this RFI. All costs associated with responding to this RFI will be solely at the interested party's expense. Not responding to this RFI, does not preclude participation in any future RFP.

2.0 Background

The NGA has an existing mission-critical need to provide Cybersecurity and Risk Management services to ensure the security of its programs and systems. Any identified Cybersecurity and Risk Management solution will play a critical role in ensuring the design, build, testing, and operation of NGA Information Technology (IT) is in compliance with Committee on National Security Systems Instructions (CNSSI) 1253, National Institute of Standards (NIST) Special Publication (SP) 800-53, Risk Management Framework (RMF), and the Intelligence Community Directive (ICD) 503.

2.1 Planned Acquisition: Full and Open Competition.

2.2 Performance:

2.2.1 Period of Performance (POP): 1 Base Year with up to 4 Option Years

2.3 Constraints and Limitations: The following Constraints and Limitations are set forth in the DRAFT PWS - TBD

2.4 Security Requirements: The services to be performed involve access to the handling of classified materials up to and including Top Secret / Sensitive Compartmented Information (TS/SCI) and must be assured of compliance with National Industrial Security Program Operating Manual (NISPOM) (DOD Directive 5220.22-M). Onsite personnel associated with performance on this contract must have a TS/SCI clearance and Counter Intelligence (CI) Polygraph.

3.0 Requested Information

Responses may contain classified information as necessary to provide meaningful comments and recommendations. All responses must include appropriate classification markings. No proprietary concepts or information should be included in the submittal. Input on the information contained in the responses may be solicited by NGA from non-Government consultants / experts who are bound by appropriate non-disclosure agreements. This document and its attachments are not to be used as sources of derivative classification.

3.1 Administrative

Information to include the following as a minimum:

3.1.1. Name, mailing address, phone number, company website, and e-mail of designated point(s) of contact.

3.1.2. Business Type: based upon North American Industry Classification System (NAICS) Code 541513 Computer Facilities Management Services applicable to this acquisition, and FAR 52.219-14, Limitation of Subcontracting, the responder is to provide answers to the following questions:

To be considered for a Small Business set-aside, at least 50 % of the cost of contract performance incurred for personnel shall be expended for employees of the responder.	**RESPONSE**	
Small Business? (FAR 19.102)	□ YES	□ NO
Small Disadvantaged small business? (FAR 19.304)	□ YES	□ NO
Service Disabled small business? (FAR 19.14)	□ YES	□ NO
8(a) small disadvantaged small business? (FAR 19.8)	□ YES	□ NO
HUBZone small business? (FAR 19.13)	□ YES	□ NO
Woman-Owned Small Business? (FAR 19.15)	□ YES	□ NO
Involved in a mentor and/or protégé program? (DFARS 219.71)	□ YES	□ NO

3.1.3 Data Universal Numbering System (DUNS) Number:

3.1.4 Commercial and Government Entity (CAGE) Code:

3.1.5 Defense Security Service (DSS) TOP SECRET facility security clearance?

3.1.6 Defense Contract Audit Agency (DCAA) or other certified cost accounting system?

Details:

3.1.7 Include additional details that are not already requested based on the constraints of the information request.

3.3 Questions

Please provide answers to the following questions, which will assist the Government in developing the Cybersecurity and Risk Management Acquisition Strategy:

3.3.1 What contract type (e.g. FFP, FPIF CPIF) does your company suggest for successful performance of this requirement?

3.3.1.1 What kind of Cybersecurity and Risk Management requirements would you recommend for successful performance of this contract type?

3.3.1.2 Do you have any recommendations regarding Governmentwide Acquisition Contracts (GWACs) or General Services Administration (GSA) Schedules that could accommodate the scope of the attached draft PWS.

3.3.2 Are there any cybersecurity and risk management services you would recommend including in the attached draft PWS given the scope provided?

3.3.3 What is the best way to measure and report on the Intelligence Community Directive (ICD) 503 process steps 4 (Assess) and step 6 (Continuous Monitoring) on a weekly basis, to understand progress and how to continually improve?

3.3.4 The Government strongly desires the shortest transition period that will ensure a seamless transition of services from the incumbents to the Cybersecurity and Risk Management Services Provider. The desired transition period will be less than 90 days.

3.3.4.1 What information would be required to enable your company to successfully meet or exceed the transition timeline requirements?

3.3.4.2 Would you recommend the addition of any information to the PWS that will better assist Industry in preparing and submitting their Startup Transition Plan?

3.3.4.3 What can the Government do to expedite the transition—both before and after contract award?

3.3.4.4 What recommendations do you have to manage transition costs?

3.3.5 From the scope described in the draft PWS:

3.3.5.1 What Service Performance Measurements and Acceptable Quality Levels would the contractor recommend to enable successful performance of this requirement?

3.3.5.2 What performance metrics and data sources does the contractor recommend?

3.3.5.3 What percentage of this work can be accomplished using support from small businesses? What barriers would there be to small business participation for this requirement?

3.3.6 Given that cybersecurity crosses all of IT and thus multiple contracts, what would your organization recommend to ensure effective cross contract communication, coordination and integration to provide optimal IT services to your customer?

3.3.7 The Government anticipates that the Cybersecurity and Risk Management contractor will be required to provide services for operations in a Cloud environment, to include those identified by the National Institute of Standards. What cybersecurity and risk management services related to cloud operation would your organization recommend given the scope of the draft attached PWS?

3.3.8 Information system development models are changing to shorten the time from development to operations (DevOps) through increased automation techniques. What cybersecurity and risk management services would your organization recommend to maintain software assurance and perform risk management in keeping with this life cycle model?

3.3.9 The Government is considering developing a Cybersecurity Innovation Cell (CIC) chartered with investigating future (5-10 years) Cybersecurity research, technology and processes. What cybersecurity and risk management services would your organization recommend to support a CIC?

3.4 Recommendations

The responder is invited to provide information and recommendations for fashioning this proposed acquisition. Recommendation areas may include the type of contract, anticipated contract terms & conditions, incentives, variations in delivery schedule, price and/or cost proposal support, and data requirements, contract pricing, and any other areas that the responder believes is relevant for the Government to achieve its stated objectives.

4.0 Responses

4.1 Interested parties are directed to respond to this RFI in a format of their choosing.

4.2 The total page count for the entire submission is limited to 25 pages of text. A page is defined as each face of an 8½” x 11” sheet with information contained within a one inch margin on all sides. Each 25-page submission shall include responses to the areas of interest outlined in Section 3.

4.3 All responses MUST BE submitted electronically via email to CyberRiskMgmt@nga.mil. RFI responses should be received by the cut-off date and time. Responses will not be accepted after the cut-off time and date stated above.

Electronic responses are due no later than **1600 hours EST on July 07, 2016**.

5.0 Meetings and Discussions –

The Government representatives may or may not choose to meet with interested parties to this RFI. These meetings would only be for clarification purposes to identify the interested parties potential capabilities.

6.0 Questions & Answers (Q&A)

Respondents are requested to only provide comments on the contents of the draft PWS and in their response to questions in the RFI.

Respondents are hereby notified that more than one Government Agency may be provided the responses for review, and the Government may utilize Federally Funded Research and Development Centers (FFRDC) and/or Support Contractors to provide technical advice on the responses. Otherwise, information submitted under this RFI will be limited only to the Cybersecurity Program Office and to the support contractors who have executed the requisite non-disclosure agreements and conflict of interest statements.

7.0 Summary

The information provided in this RFI is subject to change and is not binding to the Government. The Government has not made a commitment to procure any of the RFI requirements discussed, and release of this RFI should not be construed as such a commitment or as authorization to incur cost for which reimbursement would be required or sought. All submissions become Government property and will not be returned.

8.0 Attachments

8.1 Draft Cybersecurity and Risk Management Performance Work Statement (PWS) (U//FOUO)

National Geospatial-Intelligence Agency

Performance Work Statement

For

Cybersecurity and Risk Management

AKA: CYBERTRON

31 May 2016

DRAFT Version 10

Table of Contents

Overview

The National Geospatial Intelligence Agency (NGA) is a Department of Defense (DoD) Combat Support Agency that provides timely and accurate Geospatial Intelligence to both the DoD and Intelligence Community (IC) in support of National security objectives. A major part of this support is ensuring programs and systems are assessed and authorized as meeting the necessary security standards. It is within the newly merged offices of the Information Technology Directorate and the Office of the Chief Information Officer (CIO) that the Cybersecurity (CS) Offices resides. The CS mission is to execute the CIO-T responsibilities for securing the confidentiality, integrity, and availability of NGA data technology, processes, and people. CS performs the functions necessary by providing security oversight, risk management assessment and authorization for NGA Information Technology (IT) systems. The work is critical to ensure the design, build, testing, and operation of any NGA IT provides a secure IT environment in compliance with Committee on National Security Systems Instructions (CNSSI) 1253, National Institute of Standards (NIST) Special Publication (SP) 800-53, Risk Management Framework (RMF), and the Intelligence Community Directive (ICD) 503.

Place of Performance

[Note from the NGA Program Office: Specific Locations and the level of effort for support would be provided in the RFP, but has not been incorporated into this RFI]

The work to be performed is at the NGA facilities in the Washington Metropolitan Area (WMA); St. Louis Metro Area, Missouri; Denver Metro Area, Colorado; Dayton Metro Area, Ohio; Garland Texas; and NGA Support Teams (NSTs) CONUS and OCONUS. The Contractor shall be provided access to these facilities and will be provided with appropriate work space and supplies to perform the required tasks as described in this contract. However, due to the limited availability of NGA facility space the Contractor may be required to peform SCI work from from locations other than Government-provided facilities.

Scope

The NGA CS contractor will provide critical support to NGA CIO-T in the areas of Cybersecurity and Risk Management. The Cybersecurity (CS) Offices reports directly to and supports NGA CIO-T. The Director of CS serves as the Chief Information Security Officer, Agency's Authorizing Official (AO), and is responsible for executing the CIO-T's responsibilities for securing NGA information systems. CS is actively involved in day-to-day IT cybersecurity management and oversight for the Agency. To ensure IT systems are developed and tested not only with appropriate IT engineering standards, but also able to meet the necessary security standards, contractor support is needed for the various actions required to certify an IT system is operationally ready. These actions include risk management, assessment and authorization, compliance and reporting, and cybersecurity engineering and architecture. Actions related to ensuring cybersecurity is maintained in cloud environments, which are of particular concern in today's IT environment, is an important item for this contract.

Objective

The objective of this contract is to provide support services to the CIO-T Directorate in NGA. The support is specifically for the cybersecurity work being done within the CIO-T Directorate. The work required is related to cybersecurity management, cybersecurity risk analysis, assessment and authorization, cybersecurity engineering, and cybersecurity training. The objective of this support service contract is to assist NGA in performing the actions required for cybersecurity as the organization uses guidance of ICD 503, CNSSI 1253, and NIST SP 800-53.

Program Goals:

With this requirement NGA is seeking to:

- Support rapid and risk free implementation of the policies and procedures from ICD 503 and NIST SP 800-53.
- Increase the number of assessed and authorized IT systems meeting all required standards.
- Develop improved risk assessments that allow for decreased risk of cyber attacks on IT systems, to include systems implemented within the cloud.
- Obtaining metrics on how well NGA is doing in compliance with Federal laws, IC, and DoD policy in support of cybersecurity to ensure there is no or limited lack of compliance.
- Obtain a detailed cybersecurity training plan that can be implemented to allow for improved work in cybersecurity.
- Increased participation in the development of systems to ensure needed cybersecurity is addressed in system development.

The work in this office is divided amongst the following nine areas.

1. Cybersecurity Authorization and Assessment Services
2. Cybersecurity Risk Management Support Services
3. Cybersecurity Vulnerability Mitigation Support Services
4. Cybersecurity Risk Trade Off Analysis Services
5. CyberSecurity Blue Team
6. CyberSecurity Control Assessment
7. CyberSecurity Cyber Integration
8. CyberSecurity Software Assurance
9. Information System Security Engineering and Architecture
10. Compliance and Reporting

Assumptions and Constraints

This section defines the broad assumptions and constraints underlying this PWS, which the Contractor should consider in providing the required support for this effort.   Task specific assumptions and constraints are included within each functional task as applicable.

- NGA must follow the IC and DoD mandated policies in reference to cybersecurity utilizing the NIST Risk Management Framework.
- All contractor personnel must all have appropriate security clearances to work on this effort.

- All work will be performed in an accredited SCI Facility (Government and non-Government facilities).
- There is no requirement for any hardware, software, or telecommunications purchase under this effort. However, the contract will have the flexibility to procure these items in the event that they are necessary.

The following is a list of applicable documents for this effort:

Compliance Documents

- Clinger Cohen Act of 1996, National Defense Authorization Act for Fiscal Year 1996, Title 40, U.S.C. 1401, 10 Feb 1996.
- Committee on National Security Systems Instruction 1253, Security Categorization and Control Selection for National Security Systems, 15 Mar 2012.
- Committee on National Security Systems Instruction 4009, National Information Assurance (IA) Glossary, 26 Apr 2010, as amended.
- Committee on National Security Systems Policy 11, National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology Products, Jun 2013, as amended.
- Committee on National Security Systems Policy 22, Policy on Information Assurance Risk Management for National Security Systems, Jan 2012, as amended.
- Department of Defense (DoD) Directive 8570.01, Information Assurance (IA) Training, Certification, and Workforce Management, 15Aug 2004.
- Department of Defense Instruction 8500.01, Cybersecurity, 14 Mar 2014.
- Department of Defense Instruction 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT), 12 Mar 2014.
- E-Government Act of 2002, also known as the “Federal Information Security Management Act (FISMA) of 2002”, Title 44, U.S.C. 101.
- Executive Order 12333, United States Intelligence Activities, 4 Dec 1981, as amended.
- Executive Order 13526, Classified National Security Information, 29 Dec 2009, as amended.
- Intelligence Community Directive 503, Intelligence Community Information Technology Systems Security, Risk Management, Certification and Accreditation, 15 Sep 2008.
- Joint DoD/Intelligence Community Memorandum, Establishment of a Department of Defense (DoD)/Intelligence Community (IC) Unified Cross Domain Management Office (UCDMO), 15 Jul 2006.
- National Institute of Standards and Technology Special Publication 800-30, Guide for Conducting Risk Assessments, Sep 2012.
- National Institute of Standards and Technology Special Publication 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, Feb 2010.
- National Institute of Standards and Technology Special Publication 800-39, Managing Information Security Risk: Organization, Mission, and Information System View, Mar 2011.

- National Institute of Standards and Technology Special Publication 800-47, Security Guide for Interconnecting Information Technology Systems, Aug 2002.
- National Institute of Standards and Technology Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, Aug 2009, as amended.
- National Institute of Standards and Technology Special Publication 800-53A, Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans, Jun 2010.
- National Institute of Standards and Technology Special Publication 800-55, Performance Measurement Guide for Information Security, July 2008.
- National Institute of Standards and Technology Special Publication 800-137, Information Security Continuous Monitoring for Federal Information Systems and Organizations, Sep 2011.
- National Security Directive 42, National Policy for the Security of National Security Telecommunications and Information Systems, 5 Jul 1990.
- National Security Presidential Directive-54/Homeland Security Presidential Directive-23, Cybersecurity Policy, 8 Jan 2008.
- Office of Management and Budget Circular A-130, Management of Federal Information Resources, 28 Nov 2000, as amended.

Reference Documents

- Director of Central Intelligence Directive (DCID) 6/3 Policy, Protecting Sensitive Compartmented Information within Information Systems, 5 Jun 1999, as amended.
- NGA CIO Directives and Instructions.
- NGA Directive 8010 Information Systems Risk Management Framework (RMF), 27 Aug 2015.
- NGA Instruction 8010.8, Information Assurance Vulnerability Management, 13 Jul 2012, as amended.
- Senior Cybersecurity Roundtable (SCR) Charter
- Vulnerability Management Panel (VMP) Terms of Reference (TOR)

Work Products/Deliverables

A list of required deliverables and work product is provided within each functional support area. Examples of work products are technical reports, white papers, status reports, and other documents as requested. Deliverables shall be submitted to the Contracting Officer Representative (COR) or other designated NGA representative. Formal contract deliverables are designated as such and will require submission to both the Contracting Officer (CO) and COR and will be subject to acceptance procedures.

Staffing and Resources

[Note from the NGA Program Office: NGA has to track personnel that are 8570 compliant therefore it can be anticpated that the draft RFP will contain Contract Deliverables linked to staffing and

resources.]

The Contractor shall provide personnel possessing the skills, knowledge, training, and security clearances to perform the tasks required by this contract. Changes in staffing may result from unforeseen events (e.g. budget, executive mandates, organizational changes, technical changes, or special projects).

The Contractor shall ensure that personnel maintain any required professional certifications, accreditations and proficiency relative to their areas of expertise. Training of contractor personnel to fulfill these requirements shall be performed at contractor's expense. The Contractor shall retain documentation of such records.

A listing of the types of personnel and skill sets required for this effort are provided in the attachment.

Security Requirements

[Note from the NGA Program Office: A DD254 is not available at this time. However, the work to be perfomed under this contract will require cleared personnel and access to cleared facilities. Although the work that will be performed under this contract will be classified, NGA will make every effort to keep the RFP unclassified.]

The Contractor shall ensure all personnel are cleared to the appropriate required (TS/SCI) NGA level in accordance with DD254 (Contractor Security Classification Specifications). The Contractor shall submit, update, and maintain a current Contractor Position Roster Log. All personnel working on this contract must be US citizens.

All contractor personnel are required to take a Counterintelligence (CI) polygraph that will be coordinated with NGA security shortly after contract award. Backfill personnel are required to pass the polygraph within two months of arrival.

The Contractor shall adhere to the required Personnel Security policies. It shall be the responsibility of the Contractor to advise the Government of any security violation. Failure to do so may result in legal actions.

The Contractor shall track and report compliance with NGA security training requirements.

The Contractor shall notify the COR of any changes in access requirements for its personnel no later than one business day after any personnel change occurs. These changes include name changes, resignations, terminations, and reassignments to other contracts.

Organizational Conflict of Interest (OCI) Requirements

SPECIAL OCI CONDITIONS

a. If an offeror has a financial interest in any work performed for NGA at time of award of this contract (that could be subject to NGA's Information Assurance Authorization pursuant to ICD 503), the offeror may be ineligible for award of this contract. If an offeror is awarded this contract the Contractor, and its subcontractors who have performed work under this contract, may not acquire a financial interest in any work performed for NGA (that could be subject to NGA’s Information Assurance Authorization pursuant to ICD 503), and will be ineligible to perform such work for NGA during the maximum period of performance established by this contract.

b. For purposes of this special OCI provision, work “that could be subject to NGA’s Information Assurance Authorization pursuant to ICD 503” includes activities that are broadly defined as: performing testing, assessment or risk evaluation of information systems. The Contractor shall contact the Contracting Officer any time it has questions regarding the description of work performed for NGA “that could be subject to NGA’s Information Assurance Authorization pursuant to ICD 503.”

c. If the Contractor or an offeror does not have a financial interest in any work for NGA at time of award of this contract (that could be subject to NGA’s Information Assurance Authorization pursuant to ICD 503), an OCI may still exist; however, NGA will attempt to resolve those situations through normal mitigation efforts to the extent feasible.

d. This OCI provision applies to all prime contractors and subcontractors concerning this contract as well as parent companies and their wholly-owned subsidiaries.

e. After the maximum period of performance established by this task order has expired, the special restraints imposed by this clause shall not apply. However, potential OCIs may have been created nonetheless by performance under this contract as they relate to NGA developmental efforts. Those potential OCIs shall be resolved under normal OCI procedures.

TDY Travel Requirements

The Contractor may be required to travel to various locations both CONUS and OCONUS. All travel shall be pre-approved by the Government COR prior to obtaining any travel documents or reservations. For planning purposes, the Contractor shall assume travel will be by air and require the use of rental car and hotel. The Contractor shall estimate cost based on government per diem rates. JTFR regulations will be followed. Contractors are not allowed to charge the government for first or business classes of travel. Contractors may use frequent flier miles to upgrade travel, but will not charge these expenses to the government.

The support provided under this contract may require contact with foreign nationals both domestically and abroad and will require delivery of defense services and/or technical data to foreign nationals. The Contractor personnel are responsible for being knowledgeable and familiar with DoD/IC/NGA policy and guidance on working with foreign nationals.

Contract Status Review (CSR)

The Contractor must conduct and support quarterly CSRs to review the work being conducted under this contract. The Government reserves the right to increase or decrease the frequency of these reviews in accordance with the needs of the Government. The Contractor must submit an agenda for the meeting and provide minutes after the meeting indicating any action items and action officers. The Contracting Officer may modify the meeting schedule to accommodate special program needs. The items to be discussed at the CSRs include:

- Status of all the tasks being performed or planned within the next three months,
- Key accomplishments and problems encountered for the current month and unresolved issues from the previous months,
- Service level and Performance metrics, plan vs. actual for current month and FY to date,
- Staffing and expenditures – planned vs. actual for current month and FY to date,
- Contract administration – status of contracting actions in process,
- Key issues requiring NGA management attention,
- Productivity recommendations,
- Cost efficiency recommendations,
- Meetings.

The Contractor must support recurring status meetings, reviews, and conferences with the Government to discuss program progress, issues, and contractor recommended enhancements / improvements; identify potential problems, and resolve identified problems in accordance with the Contract Management Plan.

The Contractor must generate and deliver meeting agendas, meeting minutes, presentation materials and an action item list for each meeting, review and/or conference. The Contractor must notify the Government of its readiness prior to the start of any meeting, review, and/or conference. The Contractor must provide copies of all presentation materials to all government representatives at all meetings.

Contractor Status Reports

The Contractor shall provide a weekly status report that shall include a summary level of work performed, accomplishments made, staffing, and deliverables, work products submitted and issues needing resolution. At the end of each month, the Contractor shall submit a combined monthly status report of weeks one through four of the respective month.

The weekly status report is to include the following:

1. Summary of work completed
2. Hours charged by specific task
3. List of any problems.

Performance Management

Performance standards for this contract are presented in the Performance Requirements Summary (PRS). The rights of the Government and the remedies described in the PRS are in addition to the other rights and remedies set forth in the terms and conditions of this contract.

The Contractor shall measure and report its performance against the standards specified in the PRS and service level agreements as applicable. The Contractor may recommend revisions to the standards based on experience gained, contractor performance, and evolving requirements. Performance standard changes will be mutually negotiated between NGA and the Contractor.

The Government reserves the right to relieve the Contractor of performance requirements in cases where performance may be impacted due to circumstances beyond their control.

The Contractor shall establish and maintain a performance management system including an executed Service Level Agreement to ensure that the appropriate metrics are in place to manage, monitor, and report contract and task order performance and service levels.

The Government is providing minimal acceptable performance levels by task in the PRS. The final negotiated minimal performance levels in the PRS will be considered mandatory; performance that falls below those levels may be subject to penalties.

Records Management

The Contractor must create and maintain files that document the processing of work and other associated information pertaining to tasks performed under this contract in a format suitable for use by NGA.

Examples of what is to be included in the records files:

- Copies of all correspondence related to this contract between the Contractor and the Government,,
- All Contract work products and deliverables,
- Copies of all status reports,
- Upon completion of the contract, all records must be turned over to the Government.

Post Award Conference

The Contractor shall attend a Post Award Conference within fifteen days after contract award to assure that both Contractor and Government have a clear and mutual understanding of the contract and its requirements. The designated Contracting Officer will stablish the time and place of the conference, prepare the agenda and notify appropriate Government and Contractor representatives.

Technical Requirements

1. Cybersecurity Authorization and Assessment Services

The contractor support in this area is focused providing Authorization and Assessment (A&A) Services to include but not limited serving as a Delegated Authorizing Official Representative (DAOR) and reviewing risk trade off analysis required to recommend risk acceptance authorization decisions. The contractor will conduct risk assessments for NGA's complex IT systems for mission enhancement and for ensuring information systems are safeguarded, comply with Federal and NGA policies on cybersecurity, and provide authorization recommendations including Operational Authorization to Test (OATT), Authorization To Proceed (ATP), and Authorization To Operate (ATO).

The Contractor serves as DAORs. In this capacity, contractor acts on behalf of the Government in performing the duties required of this position. The NGA Risk Management Framework (RMF) Process is followed leading to information systems that are approved to operate with acceptable risks. Selection of appropriate security controls for information systems consider mission operations, individuals, and agency asset protection. Selection of security controls for information systems that operate in cloud environments is provided. A risk-based approach to security control selection and ensuring that the selection process considers effectiveness, efficiency, and constraints due to applicable laws, directives, executive orders, polices, standards, and regulations. Activities related to managing organizational risk (also known as the Risk Management Framework) are paramount to an effective information security program and can be applied to both new and legacy information system. The Contractor works with the Information Systems Owners (ISOs) and Information System Security Engineers (ISSEs) when categorizing information systems.

System category and security control selection includes identifying, prioritizing and determining risk impacts to missions and the information processed by the system.

The Contractor provides guidance to PMs and ISOs for securing information systems in accordance with ICD 503, CNSSI 1253, and NIST SP 800-30, 800-37, 800-39, and 800-137. The Contractor promotes an understanding and use of Enterprise Security Services (ESS) to enable consistent, efficient, and effective implementation of security in the information system.

The Contractor monitors information system Plan of Action & Milestones (POA&Ms) to confirm findings and recommendations are included, and risk mitigation strategies are implemented appropriately and within defined milestones.

Security controls, test results and recommendations, and risk mitigation strategies, are documented and included in the Body of Evidence (BOE). Security controls, recommendations, risk mitigation strategies are cost effective and support mission objectives.

The Contractor supports management and control of the NGA central repository for authorization documentation (i.e., Body of Evidence [BOE]), which is maintained using the XACTA software application. This support includes validating project registration requirements are completed.

The Contractor reviews security assessment plans to ensure they are comprehensive, well written, and appropriate for the test type (e.g., Blue Team, security control assessments). The

Contractor monitors testing and reviews Security Accessment Reports (SAR) to check that they include detailed test results, reasons for test failures, and recommend corrective actions.

The Contractor monitors assessment and authorization activities and POA&Ms to confirm actions are collaborated with NGA Cybersecurity offices, PMs, ISOs, and external agencies, if appropriate.

The Contractor provides analysis, reports, and metrics to CIO/T leadership concerning the status of the agency systems that are undergoing the NGA A&A process.

The Contractor supports developing and documenting risk assessment results using identified threats, applicable vulnerabilities, and likelihood of occurrence within the context of agency risk tolerences.

The Contractor assists in developing risk mitigation strategies, solutions and recommendations. by observing security tests and assessments, and reviewing test results.

BOE artifacts are complete, well written, and support authorization decisions.

Security testing is compliant with NGA Risk and ICD 503 security assessment requirements and other applicable references (examples TBD) and reasoning for determining compliance or non-compliance is documented.

Data and network layer diagrams of assigned systems are compliant with security standards and best practices, and the rationale for determining compliance or non-compliance is documented.

PMs and ISOs review enterprise security solutions, common controls, and enterprise security services and have incorporated them as applicable to realize program efficiencies while still achieving mission goals.

In conjuction with legacy system PMs, the Contractor evaluates the practicality of implementating enterprise security services.

The Contractor supports the Government in developing, documenting, and assessing measures and metrics related to cybersecurity assessments and risk acceptance.

The Contractor confirms that supplemental system authorization documentation, which is included in the XACTA record, is current and includes authorization decisions.

The Contractor provides guidance and recommendations concerning the impact to NGA risk management processes of new or revised IC and DoD policies, directives, and guidance.

Desired Outcomes

DAORs provide guidance to the ISO/ISO-Rep on the steps required for completing the NGA RMF process. This guidance includes, but is not limited to, providing support and assistance as needed to ensure timely and accurate documentation submission, validating completion of project registration actions; validating and approving system categorization and information type; validating security control and overlay selection, assessment types, and tailoring security controls when necessary.

BOE artifacts are reviewed and feedback provided to the ISO/ISO-Rep.

BOE artifacts are available and complete. These artifacts include, but are not limited to the System Security Plan (SSP), Security Assessment Procedures (SAP), Security Assement Report

(SAR), the POA&M, the Risk Assessment Report (RAR), the System Inventory and Installation Procedures, and the Security Assessment Procedures.

Letters recommending are generated for DAO authorization decisions (ATP, IATT and ATO with POA&M. These letters notes restrictions and risk mitigation actions as necessary.

A&A activities are accomplished following the NGA RMF workflow.

Recommendations for improving the NGA authorization processes are provided. These recommendations may include authorization actions involving CIO/T, PMs, and ISOs.

Status on the CIO/T system authorization process is easily obtained.

Detailed documentation of system risk assessments identifies the severity of the risk and the likelihood of occurence.

Legacy systems maintain or reduce accepted level of risk throughout the system lifecycle.

Legacy systems undergoing security relevant changes are migrated to the RMF.

Legacy systems evaluate use enterprise security services and where practical, implement these services.

Constraints

TBD

Work Products and Deliverables

TBD

PERFORMANCE MEASURES				
	Performance Measurement	Performance Standard	AQL	Methods of Surveillance
Cybersecurity Authorization and Assessment Services				
	TBD	TBD	TBD	TBD

ACCEPTABLE QUALITY LEVELS				
Cybersecurity Authorization and Assessment Services				
Number	Requirement	Deliverables	Constraints	Outcomes

	TBD	TBD	TBD	TBD

2. Cybersecurity Risk Management Support Services

The contractor shall serve as principal security advisor on risk matters, technical and otherwise, involving the identification and prioritization of security risks to NGA information systems. The contractor collaborates within the agency and at IC security meetings and working groups. This collaboration includes examining risk analysis and mitigation security considerations and providing critical thinking when applying security controls to systems design, implementation, and operation of NGA systems supporting IC missions.

Support for developing and documenting risk assessment results and use threats, applicable vulnerabilities, and likelihood of occurrence within the context of agency risk tolerences. The risk assessment is be prepared using NIST SP 800-30, 800-39, and NGA policies. The assessment identifies risks to NGA mission and the system’s residual risk.

Risk mitigation strategies, solutions and recommendations for information system are developed.

The Contractor validates that PMs and ISOs have reviewed enterprise security solutions, common controls, and other enterprise security services and have incorporated them as applicable to realize program efficiencies while still achieving mission goals.

The Contractor supports the Government in developing, documenting, and assessing measures and metrics related to cybersecurity assessments and risk acceptance.

The Contractor recommends participation at selected Federal, DoD, IC Information Assurance Forums, meetings and working groups and attends these meetings as requested by the government.

The Contractor provides guidance and recommendations concerning the impact to NGA risk management processes of changes to IC and DoD policies, directives, and guidance.

The Contractor coordinates and evaluates cybersecurity activities, such as program coordination and problem resolution, and ensures resource impacts are minimized.

The timeliness of implementing mandatory federal, IC and NGA security policies and procedures is improved.

Desired Outcomes

Documentation indicating system vulnerabilities and the likelihood of occurence is available.

Results of risk assessments of systems are available and identify risks and provides system residual risks.

Constraints

TBD

Work Products/ Deliverables

TBD

PERFORMANCE MEASURES				
	Performance Measurement	Performance Standard	AQL	Methods of Surveillance
Cybersecurity Risk Management Support Services				
	TBD	TBD	TBD	TBD

ACCEPTABLE QUALITY LEVELS				
Cybersecurity Risk Management Support Services				
Number	Requirement	Deliverables	Constraints	Outcomes
	TBD	TBD	TBD	TBD

3. Cybersecurity Vulnerability Mitigation Support Services

The Contractor support in this area focuses on serving as a vulnerability mitigation analyst by collecting, researching, and monitoring enterprise IT vulnerability resolution. The Contractor also serves as Secretariat for the second and third tiers of the NGA Cybersecurity Governance Hierarchy (currently identified as the Senior Cybersecurity Roundtable (SCR)(tier 2) and the Vulnerability Management Panel (VMP)(tier 3).

Vulnerability information from multiple sources and work with ISOs is collected and where possible, used to resolve system specific vulnerabilities. For those vulnerabilities requiring resources (personnel, funding, etc.) to resolve, the contractor coordinate through the Cybersecurity Governance Hierarchy as appropriate, to ensure the vulnerabilities are prioritized, fixed, mitigated, or accepted.

The Contractor provides administrative and coordination support for the VMP. Meetings of the panel are scheduled, and agendas are drafted, finalized, and distributed. The VMP information repository is maintained. Panel decisions and actions are recorded, announced and tracked as outlined in the VMP governance document (currently the VMP Terms of Reference).

The Contractor provides administrative and coordination support for the SCR. Meetings of the roundtable are scheduled, and agendas are drafted, finalized, and distributed. The SCR information repository is maintained. Panel decisions and actions are recorded, announced and tracked as outlined in the VMP governance document (currently the VMP Terms of Reference).

Information system vulnerabilities and discrepancies are tracked, and responses are coordinated with NGA and external organizations as appropriate. Vulnerabilities and discrepancies of information systems that operate in the cloud are reviewed to determine applicability to other cloud-based systems. Validation that corrective actions are implemented is completed. Corrective actions ensure vulnerabilities are mitigated and discrepancies are resolved as defined by NGA or external organizations, to include but not limited to the USCYBERCOM or the IC Security Coordination Center.

Risk mitigation strategies, recommendations, and applicable security controls are documented. This documentation includes the cost effectiveness in supporting mission goals.

Analysis, reports, and metrics to CIO/T leadership concerning the status of the agency vulnerabilities at both system and enterprise levels is provided.

Desired Outcomes

Status of agency vulnerabilities is easily obtainable from Strategic and Tactical perspectives.

Cybersecurity Governance Hierarchy (VMP and SCR) is informed, which enables Security Council strategy execution and reduces risk within the agency.

Holistic view of the enterprise IT vulnerability posture.

Reduced number of vulnerabilities in enterprise systems.

Documented actions and outcomes of efforts to eliminate, mitigate, or accept system or enterprise vulnerabilities.

Constraints

TBD

Work Product/ Deliverables

TBD

PERFORMANCE MEASURES				
	Performance Measurement	Performance Standard	AQL	Methods of Surveillance
Cybersecurity Vulnerability Mitigation Support Services				
	TBD	TBD	TBD	TBD

ACCEPTABLE QUALITY LEVELS				
Cybersecurity Vulnerability Mitigation Support Services				
Number	Requirement	Deliverables	Constraints	Outcomes
	TBD	TBD	TBD	TBD

4. Cybersecurity Risk Trade-Off Analysis Services

The Contractor support in this area focuses on providing technical support to the AO/DAO/CISO to ensure that security considerations and risk tradeoffs are integrated throughout the engineering development and operations life system cycles, and that residual risk remains at an acceptable level during the RMF continuous monitoring phase.

The Contractor participates in system development from the start of the mission need decision process through system operations to ensure security issues risk trade-off decisions are accomplished and incorporated into system designs.

The Contractor participates in system discovery or system registration processes to assist the Government in determining applicable security controls.

Coordination with internal and external Offices of Primary Responsibility (OPR) concerning technical support for system security, risk mitigation, threat and vulnerability evaluation facilitates compliance with NGA, DoD and IC directives and policies.

Interconnection Security Agreements (ISAs) and Memoranda of Understanding (MOU) documents outlining agreements with DoD and IC agencies are prepared.

The Contractor represents the Government at meetings between NGA and DoD/IC that address Cybersecurity and reports meeting results to the NGA AO/DAO/CISO. Reporting includes recommendations and impact assessments. NGA positions at said meetings are represented.

Evaluation assessment results and risk trade-off analyzes, and mitigation strategies are recommended.

Guidance, insight and comments to OPRs concerning IC, DoD, and NGA policies is provided.

The Contractor collaborates task activities and solutions within NGA and other government and industry organizations.

Cybersecurity measures and metric information and used to provide recommendations for improving the NGA A&A processes.

Desired Outcomes

System risks are documented and maintained with the A&A BOE.

ISA and MOU files are documented and maintained with the A&A BOE.

Constraints

TBD

Work Products/Deliverables

TBD

PERFORMANCE MEASURES				
	Performance Measurement	Performance Standard	AQL	Methods of Surveillance
Cybersecurity Risk Trade-Off Analysis Services				
	TBD	TBD	TBD	TBD

ACCEPTABLE QUALITY LEVELS				
Cybersecurity Risk Trade-Off Analysis Services				
Number	Requirement	Deliverables	Constraints	Outcomes
	TBD	TBD	TBD	TBD

5. Cybersecurity Blue Team

The contractor support in this area is focused on performing Blue Team Assessments and identifying vulnerabilities and security gaps in support of A&A, System Operations, and Computer Network Defense activities.

The Contractor coordinates and conducts Blue Team assessment follows within Government constraints and industry best practices.

The Contractor conducts Blue Team cyber penetration test planning, execution, tracking, and reporting activities. These activities include vulnerability research, detection, analysis, and exploitation in NGA's information systems to assess system and agency risk. The Contractor recommends countermeasures that reduce risk to systems and the Agency.

The Contractor provides an assessment of the degree to which a system is compliant with the operating system, network, and application security the DoD Security Technical Implementation Guide (STIG) reviews, NGA / IC policies and guidelines, NSA recommendations, and security best practices.

The Contractor employs tools and techniques that identify vulnerabilities and shortcomings of the system or systems under assessment. These tools and techniques will follow government and industry best practices within the limits of polices and guidance. The tools and techniques could include, but are not limited to manual test procedures or analysis, web assessment software, vulnerability scanning tools, penetration test tools, and or Contractor developed custom scripts. Tests may be conducted on the systems remotely or locally to facilitate access to the system and to identify security vulnerabilities, risks, threats, and gaps.

Upon completion of each Blue Team engagement, the Government is apprised of the processes employed in the assessment, findings and analysis of the findings. The Contractor also provides the Government corrective actions in order to reduce risk. The Government PM and ISO, vulnerability management office; and the appropriate Computer Network Defense Service Provider (CNDSP) receive this information. The root-cause of of technical and non-technical findings, and additional information as necessary to enable understanding the functions are provided. Methods to reduce repeated findings in the systems under test and other Government systems are provided. Methods of identifying the source of failures / successes with policy compliance; deviation from organizational processes and procedures; and need for agency resources are shared.

The Contractor provides technical support to NGA's Computer Network Defense Service Provider (CNDSP) and counter-intelligence components to assist comprehensive incident handling and forensic analysis of compromised systems with, and provides technical subject matter expertise (SME) in the areas of network exploitation and evasion techniques.

The Contractor develops custom scripting that support Blue Team objectives, NGA mission needs and assist NGA System Administrators and / or the CNDSP components in discovering vulnerabilities. Scripting tools are developed using languages that could include are but not limited to: python, powershell, bash, and batch.

The Contractor provides SCAs technical assistance as needed in the areas of test plan development and security control testing specific to security boundaries, to include Cross Domain Solutions (CDS).

The Contractor provides technical augmentation as needed to the Cross Domain Support Element (CDSE) to identify weaknesses in NGA CDSss.

The Contractor supports CIO/T objectives and positions at internal and external information security and cyber defense meetings, conferences, technical exchange meetings and working groups. Following conclusion of these meetings, the Contractor communicates meeting results to the Government. This communications includes action items for the CIO/T organization.

The Contractor participates in developing and maintaining Blue Team documentation that could include, but is not limited to: Standard Operating Procedures (SOPs); Concept of Operations (CONOPs); white papers; technical documentation; status reports; daily operations and processes; weekly activity reports; summaries; briefings; trip reports; handouts and manuals; correspondence; responses to NGA action items and taskings, and other documentation as specified by the government (CDRL B001). The content and format of all documentation is subject to the review and approval of the Government.

Desired Outcomes

Blue Team Assessment reports include test findings, recommendations and supporting information.

CIO/T senior managers, CISO, CNDSP components, and ISOs are provided information on Blue Team test results.

Blue Team test results are detailed, comprehensive, and complete. Test results are easily accessible by CIO/T managers and the CISO.

Root-causes of findings are identified and actionable remediation steps provided so future discoveries of the same issue are reduced.

Contractor attendance at meetings and conferences at which NGA is represented government objectives for the meeting are achieved.

Constraints

TBD

Work Products/Deliverables

TBD

PERFORMANCE MEASURES				
	Performance Measurement	Performance Standard	AQL	Methods of Surveillance
Cybersecurity Blue Team				

	TBD	TBD	TBD	TBD

ACCEPTABLE QUALITY LEVELS				
Cybersecurity Blue Team				
Number	Requirement	Deliverables	Constraints	Outcomes
	TBD	TBD	TBD	TBD

6. Cybersecurity Control Assessment

The contractor support in this area is focused performing Security Control Assessments (SCA), which are an integral part of the Assessments and Authorization process.

The Contactor performs detailed assessments of the security controls that have been identified and implemented for Systems as a part of the NGA Risk Management Framework Process. The The results of these assessments are documented in a Security Assessment Report (SAR). The SAR includes an evaluation of the assessment results, identification of weaknesses or deficiencies, and recommendations for corrective actions to mitigate system risk.

SCAs determine residual security risks on host, network applications, and mobile device and mobile applications. The SAR is provided to the DAO, ISSE and PM and includes an analysis of the system's security control compliance, and technical and non-technical findings. Recommendations concerning authorization approval or denial are presented to the appropriate authorization official. Rationale for these recommendations is provided.

The Contractor performs host, network, cloud, application based security control assessments, determines residual security risks, prepares assessment test reports, prepares and assesses test plans, and provides formal recommendations to support authorization decisions.

The Contractor assesses system compliance with operating system, network, and application security guidance DoD Security Technical Implementation Guides (STIG).

The Contractor employs test plans and test procedures tailored to the security controls of the system under test. The tools and techniques could include, but are not limited to manual test procedures or analysis, web assessment software, vulnerability scanning tools, penetration test tools, and or Contractor developed custom scripts.

System security plans are reviewed and feedback is provided to ISOs. These reviews provide information related to the security controls being assessed. Assessments are contucted in accordance with applicable NGA, DoD, and IC policies and guidelines.

Detailed test plans are prepared for assessing security testing of security controls specific to security boundaries and enterprise controlled interfaces, to include Cross Domain Solutions (CDS). Assessments of these critical enterprise systems are performed and a SAR prepared with the results.

The Contractor supports the NGA Cross Domain Support Element in identifying weaknesses in NGA CDSs.

The Contractor supports on-site and remote testing of Federal Information Security Management Act (FISMA) requirements. Tools and techniques for performing FISMA tests could include manual testing, vulnerability scans, and penetration testing. FISMA testing is performed at industrial and NGA hosted sites in both the Continental United States (CONUS) and Outside Continental United States (OCONUS).

The Contractor participates in developing and maintaining SCA documentation that could include, but is not limited to: Standard Operating Procedures (SOPs); Concept of Operations (CONOPs); white papers; technical documentation; status reports; daily operations and processes; weekly activity reports; summaries; briefings; trip reports; handouts and manuals; correspondence; responses to NGA action items and taskings, and other documentation as specified by the government (CDRL B001). The content and format of all documentation is subject to the review and approval of the Government.

SCA test plans and procedures, and the SAR are presented in a consistent format to facilitate review and understanding by DAORs, SIOs, and CIO/T personnel.

The Contractor supports CIO/T objectives and positions at internal and external information security and cyber defense meetings, conferences, technical exchange meetings and working groups. Following conclusion of these meetings, the Contractor communicates meeting results to the Government. This communication includes action items for NGA.

Desired Outcomes

SARs document assessment results and recommend corrective actions.

CIO/T senior managers, CISO, CNDSP components, and ISOs are provided information on SCA test results.

SCA test results are detailed, comprehensive, and complete. Test results are easily accessible by CIO/T managers and the CISO.

Attendance at meetings and conferences where the Contractor represents NGA meets government objectives for the meeting are achieved and actions are documented.

Constraints

TBD

Work Products/Deliverables

TBD

PERFORMANCE MEASURES				
	Performance Measurement	Performance Standard	AQL	Methods of Surveillance
Cybersecurity Control Assessment				
	TBD	TBD	TBD	TBD

ACCEPTABLE QUALITY LEVELS
Cybersecurity Control Assessment

Number	Requirement	Deliverables	Constraints	Outcomes
	TBD	TBD	TBD	TBD

7. Cybersecurity Cyber Integration

The contractor support in this area is focused on inserting cyber into all aspects/programs at NGA.

The Contractor develops and methods to identify, collect, process, manage, and analyze large volumes of data to build and enhance NGA's cyber assessments.

The Contractor performs data mining and retrieval, applies statistical and mathematical analyses to identify trends, solve analytical problems, optimize performance, and gathers intelligence using a range of commercial and open-source tools. Analysis of transistions to cloud environments is performed.

The Contractor communicates analytical judgements through appropriate reporting channels. The contractor participates in the production of reports or metrics that convey information and findings through methods that could include, but are not limited to written communication, advanced data visualization techniques, and dashboards.

The Contractor develops tools to support Cyber Integration mission requirements and produce meaningful statistical modeling and analytical deliverables. Scripting languages could include, but are not limited to Python, R, and JavaScript.

The Contractor provides recommendations and guidance for improvements for the Cyber Integration program.

The Contractor supports CIO/T objectives and positions at internal and external information security and cyber defense meetings, conferences, technical exchange meetings and working groups. Following conclusion of these meetings, the Contractor communicates meeting results to the Government. This communication includes action items for NGA as appropriate.

The Contractor participates in developing and maintaining Cyber Integration documentation that could include, but is not limited to: Standard Operating Procedures (SOPs); Concept of Operations (CONOPs); white papers; technical documentation; status reports; daily operations and processes; weekly activity reports; summaries; briefings; trip reports; handouts and manuals; correspondence; responses to NGA action items and taskings, and other documentation as specified by the government (CDRL B001). The content and format of all documentation is subject to the review and approval of the Government.

Special Project:

A Cyber Innovation Cell (CIC) is being developed to advance NGA's cybersecurity implementation, reduce security risk, and achieve efficiencies. Support for implementing CIC infrastructure and concepts is provided.

Desired Outcomes

Cyber Integration project results are documented and cybersecurity issues identified in the documentation.

CIO/T senior managers, CISO, CNDSP components, and ISOs are provided information on SCA test results.

SCA test results are detailed, comprehensive, and complete. Test results are easily accessible by CIO/T managers and the CISO.

Attendance at meetings and conferences where the Contractor represents NGA meets government objectives for the meeting are achieved and actions are documented.

Constraints
TBD

Work Products/Deliverables
TBD

PERFORMANCE MEASURES				
	Performance Measurement	Performance Standard	AQL	Methods of Surveillance
Cybersecurity Cyber Integration				
	TBD	TBD	TBD	TBD

ACCEPTABLE QUALITY LEVELS				
Cybersecurity Cyber Integration				
Number	Requirement	Deliverables	Constraints	Outcomes
	TBD	TBD	TBD	TBD

8. Cybersecurity Software Assessment

Contractor support in this area is focused on performing Software and Application Assessments, which are an integral part of the A&A process.

The Contractor performs application level security assessments, determines residual security risks, prepares assessment test plans and test reports, and provides formal recommendations to support authorization decisions.

The Contractor performs mobile device and mobile application security reviews and documents these reviews. The documentation identifies risks associated with using the device or application within NGA. Reviews of cloud related software and infrastructure and the risk of operating this software in this environment are completed.

The Contractor coordinates software assessment activities in accordance with Government approved standard operating procedures and guidelines.

The Contractor participates in the software discovery and/or software registration processes to assist the Government in determining applicable security controls.

The Contractor coordinates with internal and external OPRs concerning technical support for software security, risk mitigation, threat and vulnerability evaluation to ensure compliance with NGA, DoD and IC directives and policies.

The Contractor provides recommendations for improving software and application assessment processes.

The Contractor develops and documents a software risk assessment context that includes, but is not limited to identifying threats, applicable vulnerabilities, and likelihood of occurrence. Risk assessments are prepared using NIST SP 800-53 and the NGA RMF process. The assessment identifies risks to NGA missions.

The Contractor participates in developing and maintaining software and application assessment documentation could include, but is not limited to: Standard Operating Procedures (SOPs); Concept of Operations (CONOPs); white papers; technical documentation; status reports; daily operations and processes; weekly activity reports; summaries; briefings; trip reports; handouts and manuals; correspondence; responses to NGA action items and taskings, and other documentation as specified by the government (CDRL B001). The content and format of all documentation is subject to the review and approval of the Government.

The Contractor supports CIO/T objectives and positions at internal and external information security and cyber defense meetings, conferences, technical exchange meetings and working groups. Following conclusion of these meetings, the Contractor communicates meeting results to the Government. This communication includes action items for NGA.

In support of the NGA Software Approval Process (SWAP), the Contractor shall:

- Review open-source and other critical software to make a risk determination associated with its potential use and provide risk acceptance recommendations to the Delegated Authorizing Official (DAO);
- Review and prepare reports of vulnerabilities related to the potential use of the reviewed software;

- Review and update all SWAP SOPs, Work Instructions, MOAs, and CONOPS as changes occur with official versions published semi-annually.

Desired Outcomes

CIO/T senior managers, CISO, CNDSP components, and ISOs are provided information on software and application assessment test results.

Software and application assessment test results are detailed, comprehensive, and complete. Test results are easily accessible by CIO/T managers and the CISO.

Attendance at meetings and conferences where the Contractor represents NGA meets government objectives for the meeting are achieved and actions are documented.

Comprehensive documentation of software testing strategies, plans, procedures, and identified risk is prepared.

Recommentations for an agile, streamlined and repeatable process for software ingest and usage are provided.

Constraints

TBD

Work Products/Deliverables

TBD

PERFORMANCE MEASURES				
	Performance Measurement	Performance Standard	AQL	Methods of Surveillance
Cybersecurity Software Assessment				
	TBD	TBD	TBD	TBD

ACCEPTABLE QUALITY LEVELS				
Cybersecurity Software Assessment				
Number	Requirement	Deliverables	Constraints	Outcomes

	TBD	TBD	TBD	TBD

9. Information System Security Engineering (ISSE) and Architecture

The contractor support in this task area is focused on providing information system security engineering support to ISOs. Considered within this area are applying best practices and processes for capturing, refining, and assisting in prioritization of security requirements based on risk, engineering principles, and mission requirements.

Support to the ISOs to understand and develop system requirements and technical options for cybersecurity engineering based on the system architectures is provided. The Contractor provides risk mitigation alternatives.

The Contractor participates in design, development, and implementation of information systems to ensure these systems implement security controls applicable to the system and are in compliance with required security features and safeguards. Support for information systems being migrated or developed for cloud environments is provided.

IA policies, procedures, and requirements are analyzed and recommendations are provided to ISOs to support the development of interoperable, standard, and secure systems.

The Contractor works with the SCAs in the engineering design phase to understand the security controls of the system, security tradeoffs, and other relevant information.

Working with the Government, cost/benefit analysis on implementing system security design functions are provided.

The Contractor performs security engineering analysis and documentation reviews to ensure that Government IA policies, procedures and requirements have been met or justified and tracked. Risk mitigations activities are be documented in the system Plan of Action and Milestones (POA&M). These reviews are documented and provided to the government.

The Contractor provides the Government with technical guidance during security design reviews.

Potential solutions to security issues are provided to the Government. Vendor documentation is a source for information when developing these solutions.

NIST Special Publications (SP) are reviewed quarterly to ensure all NGA information systems and networks are in compliance with SPs.

The Contractor provides the Government PM a weekly report that identifies significant security issues and events.

The Contractor provides network engineering support for the strategic defense of NGA network infrastructures and operations against compromise due to connections of networks at different security levels.

The Contractor provides recommendations and guidance for implementing security features and safeguards throughout a systems life cycle.

The Contractor provides guidance on security control selection and implementation to CDS developers.

The Contractor provides technical support to the NGA CDSE.

The Contractor provides guidance and recommendations for integrating cybersecurity requirements during information system continuity planning.

The Contractor reviews Disaster Recovery and Continuity of Operation Plans (COOP) and provides recommendations for ensuring these plans are executable in the system's operational environment.

The Contractor develops tests to ensure Disaster Recovery and COOP Plans are feasible and provides written recommendations to increase the effectiveness of the plans.

Desired Outcomes

Cybersecurity requirements are included in all stages of the system's life cycle process.

Disaster Recovery and COOP plans work as required and written recommendations are provided to increase the effectiveness of these plans.

NGA IT systems are in compliance with System Security Plans.

Security engineering analysis reviews are documentated of are provided to ensure Government IA policies, procedures and requirements have been met or POA&Ms are developed.

Constraints

TBD

Work Products/Deliverables

TBD

PERFORMANCE MEASURES				
	Performance Measurement	Performance Standard	AQL	Methods of Surveillance
Information System Security Engineering (ISSE) and Architecture				
	TBD	TBD	TBD	TBD

ACCEPTABLE QUALITY LEVELS				
Information System Security Engineering (ISSE) and Architecture				
Number	Requirement	Deliverables	Constraints	Outcomes

	TBD	TBD	TBD	TBD

10. Compliance and Reporting

Contractor support in this area is focused on gathering metrics throughout NGA to ensure the agency is in compliance with Federal laws and IC/DoD requirements, to including FISMA, ICD 503, DODD 8140.01, and other policies. The underlying emphasis is enterprise level improvement of security posture through decision-making based on quality data and assessment/analysis.

The Contractor works across cybersecurity components to submit, respond, and compile Directors Action Committee taskers.

The Contractor assesses the NGA Cyber Assurance program against industry best practice .

As requested by the Government PM, the Contractor provides periodic status briefings on network and systems assessments progress, findings, and remediation efforts.

The Contractor prepares the annual FISMA report for the Agency, which includes both narrative and metric sections.

The Contractor prepares quarterly FISMA metric updates based on available information. These updates are delivered to DNI CIO POCs using automated means. .

Computer Network Defense (CND) reports are prepared annually or when required by DoD.

An internal NGA Top Ten Vulnerability Listing (TVL) and Agency-Level Plan of Action and Milestones (ALP) reports are developed. The Vulnerability Management Process (VMP) is a source of information for developing these products for quarterly submission.

NGA internal Enterprise Readiness Cell weekly and quarterly reports are developed.

Joint Force Readiness Review (JFRR) reports are prepared. NGA Mission Essential Tasks (AMET) information is available for use in report generation on a quarterly basis or as required by DoD. A consolidated and Key Component (KC) Director-approved AMET readiness assessment using the NGA AMETL Assessment Worksheet is developed in collaboration with. Supporting office(s).

The Contractor provides support information for tri-annual CNDSP audits. This information includes continuous readiness measures and a listing security controls used for the Evaluator Scoring Metrics (ESM) checklist, which judges compliance of Standard Operating Procedures (SOPs) and Work Instruction (WIs).

The Contractor conducts a Documentation Control Board supporting CNDSP audit readiness. This board reviews support documentation and maintains the documentation under configuration and revision control.

The Contractor develops and maintains an Operating Documentation Library that stores Cyber Work Instructions, Standard Operating Procedures and Policies. This library will support CNDSP, FISMA, FISCAM, and other higher headquarters inspections. Documents are reviewed before entry to the library, stored under configuration and version control, and are reviewed annually.

The Contractor supports CIO/T objectives and positions at internal and external information security and cyber defense meetings, conferences, technical exchange meetings and working groups. Following conclusion of these meetings, the Contractor communicates meeting results to the Government. This communication includes action items for NGA. The Contractor prepares the monthly IA metrics report.

The Contractor supports semi-annual updates to the IA Strategic Plan, IA Implementation Plan, and NGA's IA policies and instructions.

The Contractor leads, supports or facilitates Agency-level, directorate-level, Office-level, and Division level security assessments of NGA's information systems, networks, and remediation of IA vulnerabilities identified as a result of those assessments. As a result of these security assessments, at these same organizational levels, security assessments of NGA's enterprise security posture, mitigation of IA findings, and risks are identified.

Support for NGA's IA Program is provided. This support includes developing, collecting, assessing, and reporting IA metrics; and developing, implementing and maintaining Agency-level information assurance plans and documents. The contractor develops, implements, and executes Agency or Office level IA special programs or projects as required.

Support for FISMA site visits is provided. This support includes planning, execution, and reporting the site visits. Assistance in preparing annual site visit budget estimates for conducting these site visits is also provided.

Desired Outcomes

NGA required reports for FISMA, JFRR, CND, TTV, ALP, ITEC Briefing, Enterprise Readiness Cell, etc. are submitted within required milestones and include accurate information.

Constraints

TBD

Work Products/Deliverables

TBD

PERFORMANCE MEASURES				
	Performance Measurement	Performance Standard	AQL	Methods of Surveillance
Compliance and Reporting				
	TBD	TBD	TBD	TBD

ACCEPTABLE QUALITY LEVELS
Compliance and Reporting

Number	Requirement	Deliverables	Constraints	Outcomes
	TBD	TBD	TBD	TBD

Acronyms

A&A	Assessment and Authorization
AO	Authorizing Official
ATP	Authority to Proceed
ATO	Authority to Operate
CFTE	Contractor Full Time Equivalent
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CS	Cybersecuirty Office within the NGA CIO Office
CND	Computer Network Defense
CNSS	Committee on National Security Systems
COR	Contract Officer Representative
DAO	Delegated Authorizing Official
DOD/DoD	Department of Defense
FAR	Federal Acquisition Regulation
FISMA	Federal Information Security Management Act
FTE	Full Time Equivalent
IA	Information Assurance
IAVM	Information Assurance Vulnerability Management
ICVM	Intelligence Community Vulnerability Management
ICD	Intelligence Community Directive
ISSE	Information System Security Engineer
IT	Information Technology
KC	Key Components
KISSI	Key Information Sharing and Safeguarding Indicators
NGA	National Geospatial-Intelligence Agency
NIST	National Institute of Standards and Technology
NMR	Noncompliance Machine Report
NSG	National System for Geospatial Intelligence
OAT	Operational Authority to Test
OCI	Organizational Conflict of Interest
OCIO	Office of the Chief Information Officer

OPR	Office of Primary Responsibility
PM	Program Manager
POA&M	Plan of Action and Milestones
RMF	Risk Management Framework
SAR	Security Assessment Report
SCA	Security Control Assessment/Security Controls Assessors
SE	System Engineering
SP	Special Publication
STIG	Security Technical Implementation Guide
TC	Technical Compliance
TDY	Temporary Duty

- .

Risk Table

Sample of the types of Tables used in Identification of risk due to Adversaries and Non-Adversarial threats.

1	2	4	5	6	7	8
Threat Event	Threat source	Likihood of attack Initiation	Vulnerabilities/ Predisposing characteristics	Likelihood that Initiated Attack Succeeds	Overall Likelihood	Consequences /Affected Assets