DRAFT
Attachment E
TASK ORDER REQUEST (TOR)

for

Cyberspace Operations Support Services

in support of:

United States Cyber Command (USCYBERCOM)

NOTE: Section B of the Contractor's multiple award (MA) Indefinite Delivery/Indefinite Quantity (IDIQ) is applicable to this Task Order (TO) and is hereby incorporated by reference. In addition, the following applies:

B.1 GENERAL

The work shall be performed in accordance with all Sections of this TO and the contractor's Basic Contract, under which the resulting Task Order (TO) will be placed. An acronym listing to support this Task Order Request (TOR) is included in Section J (Attachment I).

B.2 ORDER TYPES

The contractor shall perform the effort required by this TO on a Cost-Plus-Fixed-Fee (CPFF) basis for Contract Line Item Numbers (CLINs) 0001, 0002, 0003, 1001, 1002, 1003, 2001, 2002, 2003, 3001, 3002, 3003, 4001, 4002, 4003 and Not-to-Exceed (NTE) basis for CLINs 0004, 0005, 0006, 1004, 1005, 1006, 2004, 2005, 2006, 3004, 3005, 3006, 4004, 4005, and 4006.

B.3 SERVICES AND PRICES/COSTS SCHEDULE

All CPFF CLINs are TERM and CPFF CLIN work will end based on the period of performance (PoP).

Long-distance travel is defined as travel over 50 miles from the contractor employee's duty station. Local travel will not be reimbursed.

The following abbreviations are used in this price schedule:

CLIN	Contract Line Item Number
CPFF	Cost-Plus-Fixed-Fee
NTE	Not-to-Exceed
ODC	Other Direct Cost

B.3.1 BASE PERIOD

MANDATORY CPFF LABOR CLIN

CLIN	Description	Level of Effort/ # of Hours	Cost	Fixed Fee	Total Cost Plus Fixed Fee
0001	Labor (Tasks 1-7, excluding Subtasks 2.2, 2.7, 6.2, 7.4, 7.5)		$	$	$

OPTIONAL CPFF LABOR CLINs

CLIN	Description	Level of Effort/ # of Hours	Cost	Fixed Fee	Total Cost Plus Fixed Fee
0002	Labor (Subtasks 2.2,2.7,6.2,7.4, & 7.5)		$	$	$
0003	Labor (Task 8)		$	$	$

COST REIMBURSEMENT TRAVEL, TOOLS and ODC CLINs

CLIN	Description		Total Ceiling Price
0004	Long-Distance Travel Including Indirect Handling Rate up to _____%	NTE	$100,000
0005	Tools Including Indirect Handling Rate up to _____%	NTE	$75,000
0006	ODCs Including Indirect Handling Rate up to _____%	NTE	$20,000

TOTAL BASE PERIOD CLINs: **$_____**

B.3.2 FIRST OPTION PERIOD:

MANDATORY CPFF LABOR CLIN

CLIN	Description	Level of Effort/ # of Hours	Cost	Fixed Fee	Total Cost Plus Fixed Fee
1001	Labor (Tasks 1-7, excluding Subtasks 2.2, 2.7, 6.2, 7.4, 7.5)		$	$	$

OPTIONAL CPFF LABOR CLIN

CLIN	Description	Level of Effort/ # of Hours	Cost	Fixed Fee	Total Cost Plus Fixed Fee
1002	Labor (Subtasks 2.2,2.7,6.2,7.4, & 7.5)		$	$	$
1003	Labor (Task 8)		$	$	$

COST REIMBURSEMENT TRAVEL, TOOLS and ODC CLINs

CLIN	Description		Total Ceiling Price
1004	Long-Distance Travel Including Indirect Handling Rate up to _____%	NTE	$100,000
1005	Tools Including Indirect Handling Rate up to _____%	NTE	$75,000
1006	ODCs Including Indirect Handling Rate up to _____%	NTE	$20,000

TOTAL FIRST OPTION PERIOD CLINs: $_____

B.3.3 SECOND OPTION PERIOD:

MANDATORY CPFF LABOR CLIN

CLIN	Description	Level of Effort/ # of Hours	Cost	Fixed Fee	Total Cost Plus Fixed Fee
2001	Labor (Tasks 1-7, excluding Subtasks 2.2, 2.7, 6.2, 7.4, 7.5)		$	$	$

OPTIONAL CPFF LABOR CLIN

CLIN	Description	Level of Effort/ # of Hours	Cost	Fixed Fee	Total Cost Plus Fixed Fee
2002	Labor (Subtasks 2.2,2.7,6.2,7.4, & 7.5)		$	$	$
2003	Labor (Task 8)		$	$	$

COST REIMBURSEMENT TRAVEL, TOOLS and ODC CLINs

CLIN	Description		Total Ceiling Price
2004	Long-Distance Travel Including Indirect Handling Rate up to _____%	NTE	$100,000
2005	Tools Including Indirect Handling Rate up to _____%	NTE	$75,000
2006	ODCs Including Indirect Handling Rate up to _____%	NTE	$20,000

TOTAL SECOND OPTION PERIOD CLINs: $_____

B.3.4 THIRD OPTION PERIOD:

MANDATORY CPFF LABOR CLIN

CLIN	Description	Level of Effort/ # of Hours	Cost	Fixed Fee	Total Cost Plus Fixed Fee
3001	Labor (Tasks 1-7, excluding Subtasks 2.2, 2.7, 6.2, 7.4, 7.5)		$	$	$

OPTIONAL CPFF LABOR CLIN

CLIN	Description	Level of Effort/ # of Hours	Cost	Fixed Fee	Total Cost Plus Fixed Fee
3002	Labor (Subtasks 2.2,2.7,6.2,7.4, & 7.5)		$	$	$
3003	Labor (Task 8)		$	$	$

COST REIMBURSEMENT TRAVEL, TOOLS and ODC CLINs

CLIN	Description		Total Ceiling Price
3004	Long-Distance Travel Including Indirect Handling Rate up to _____%	NTE	$100,000
3005	Tools Including Indirect Handling Rate up to _____%	NTE	$75,000
3006	ODCs Including Indirect Handling Rate up to _____%	NTE	$25,000

TOTAL THIRD OPTION PERIOD CLINs: $_____

B.3.5 FOURTH OPTION PERIOD:

MANDATORY CPFF LABOR CLIN

CLIN	Description	Level of Effort/ # of Hours	Cost	Fixed Fee	Total Cost Plus Fixed Fee
4001	Labor (Tasks 1-7, excluding Subtasks 2.2, 2.7, 6.2, 7.4, 7.5)		$	$	$

OPTIONAL CPFF LABOR CLIN

CLIN	Description	Level of Effort/ # of Hours	Cost	Fixed Fee	Total Cost Plus Fixed Fee
4002	Labor (Subtasks 2.2,2.7,6.2,7.4, & 7.5)		$	$	$
4003	Labor (Task 8)		$	$	$

COST REIMBURSEMENT TRAVEL, TOOLS and ODC CLINs

CLIN	Description		Total Ceiling Price
4004	Long-Distance Travel Including Indirect Handling Rate up to _____%	NTE	$100,000
4005	Tools Including Indirect Handling Rate up to _____%	NTE	$75,000
4006	ODCs Including Indirect Handling Rate up to _____%	NTE	$20,000

TOTAL FOURTH OPTION PERIOD CLINs: $_____

GRAND TOTAL ALL CLINs: $_____

B.4 INDIRECT/MATERIAL HANDLING RATE

Long Distance Travel, Tools, and ODC costs incurred may be burdened with the contractor's indirect/material handling rate in accordance with the contractor's disclosed practices.

a. If no indirect/material handling rate is allowable in accordance with the contractor's disclosed practices, no indirect/material handling rate shall be applied to or reimbursed on these costs
b. If no rate is specified in the basic contract, no indirect rate shall be applied to or reimbursed on these costs
c. If no rate is specified in the schedule of prices above, no indirect rate shall be applied to or reimbursed on these costs

The indirect handling rate over the term of the TO shall not exceed the rate specified in the schedule of prices above.

B.5 DIRECT LABOR RATES

Labor categories proposed shall be mapped to existing multiple award (MA) Indefinite Delivery Indefinite Quantity (IDIQ) labor categories.

B.6 INCREMENTAL FUNDING LIMITATION OF GOVERNMENT'S OBLIGATION

Incremental funding in the amount of $***,***,*** for CLINs 0001, 0002, 0003, 0004, 0005, 0006 is currently allotted and available for payment by the Government. Additional incremental funding for these CLINs will be allotted and available for payment by the Government as the funds become available. The estimated PoP covered by the allotments for the mandatory CLINs is from award through ** months of the base period, unless otherwise noted in Section B.3. The TO will be modified to add funds incrementally up to the maximum of $***,***,*** over the PoP of this TO. These allotments constitute the estimated cost for the purpose of Federal Acquisition Regulation (FAR) Clause 52.232-22, Limitation of Funds, which applies to this TO on a CLIN-by-CLIN basis.

When the work required under any CLIN is completed, and that work is within the total estimated cost shown above, the contractor shall be entitled to payment of fixed fee for that CLIN. The contractor may present, with its monthly vouchers for costs, a fee voucher in an amount bearing the same percentage of fixed fee as the certification of incurred costs bears to the total estimated cost for each CLIN. However, after payment of 85 percent of the fixed fee for the total TO, the Contracting Officer (CO) may withhold further payment of fixed fee until a reserve shall have been set aside in an amount which the CO considers necessary to protect the interest of the Government. This reserve shall not exceed 15 percent of the total fixed or $100,000, whichever is less.

Incremental Funding Chart - See **Section J, Attachment A**.

C.1 BACKGROUND

The United States Cyber Command (USCYBERCOM) Directorate of Operations (J3) establishes and provides cyber warfare capabilities to meet both deterrent and defensive National Security objectives. The J3 optimizes planning, integration, coordination, execution and force management of the cyber warfare mission in support of (ISO) the Joint warfighter. The J3 provides situational awareness of adversary attack opportunities and exercises operational and tactical control of cyber forces and capabilities, as directed. Currently, the J3 is organizationally divided into a Current Operations and Future Operations construct. Current Operations encompasses operating and defending the Department of Defense (DoD) Information Network (DODIN) and includes the Fires & Effects Division, which manages both the Joint Fires Process and the Joint Targeting Cycle and is responsible for publishing a daily Cyberspace Tasking Order (CTO) via the USCYBERCOM Command and Control (C2) portal. Future Operations spans planning for a range of potential activities from those impacting DoD information networks to those with regional and/or global implications. USCYBERCOM operates in a dynamic and changing environment and must remain flexible to achieve its mission.

C.2 SCOPE

This TO provides Cyberspace Operations support services to USCYBERCOM. This TO falls within the scope of the following IDIQ core disciplines:

1. Cyberspace Operations
2. Cyberspace Planning
3. Cyberspace Training & Exercises
4. Strategy/Policy/Doctrine Development and Campaign Assessments
5. Information Technology/Communications (IT/Comms)
6. Business Area Support and Project Management
7. Engagement Activities

Key areas to be performed within the scope of this TO include, but are not limited to:

1. Provide Mission Essential coverage to support Cyberspace Operations
2. Identify requirements and concept of operations (CONOPS) that focus on the execution of DODIN Operations and Defensive Cyberspace Operations Internal Defensive Measures (DCO-IDM) and assist in the development, synchronization, integration, and assessment of operational standards ISO achieving the Joint Information Environment (JIE) end-state
3. Contribute to efforts to secure, operate, and defend the DODIN and its critical dependencies in order to (IOT) provide full spectrum Cyberspace Operations, ensuring freedom of maneuver in that domain and denying our adversaries the same
4. Contribute to USCYBERCOM strengthening relationships with key partner nations, coordinating, synchronizing, deconflicting, and integrating operational planning efforts for full spectrum Cyberspace Operations
5. Plan, coordinate, and deconflict Offensive Cyberspace Operations (OCO), DCO, and DODIN Operations throughout the entire Joint Operational Planning Process (JOPP)

6. Identify requirements to fill gaps and identify capabilities IOT achieve an effect in accordance with (IAW) tactical objectives, operational goals, and strategic end-states
7. Prepare Courses of Action (COAs), to include advanced level targeting, capabilities pairing, and operational assessments

C.3 OBJECTIVE

The objectives of this TO are as follows:

1. Define and analyze cyberspace capabilities needed and Cyberspace Operations to meet both deterrent and decisive National Security objectives
2. Conduct planning, integration, coordination, and execution, of the Cyberspace Operations mission ISO the Joint warfighter
3. Receive, track, and resolve cyber issues and provide input to the Commander Situational Awareness Reports of Cyberspace Operations

C.4 TASKS

C.4.1 TASK 1 – PROVIDE TASK ORDER PROJECT MANAGEMENT

The contractor shall provide TO project management support. This includes the management and oversight of all activities performed by contractor personnel, including subcontractors, to satisfy the requirements identified in this Performance Work Statement (PWS). The TO project management support also includes identifying and coordinating cross-Directorate projects to ensure consistency of progress towards accomplishing the project goals. The contractor shall identify a Project Manager (PM) by name who shall provide management, direction, administration, quality assurance, and leadership of the execution of this TO.

C.4.1.1 SUBTASK 1.1 – COORDINATE A PROJECT KICK-OFF MEETING

The contractor shall schedule, coordinate, and host a Project Kick-Off Meeting **(Section F.3, Deliverable 01)** at the location approved by the Government. The meeting will provide an introduction between the contractor personnel and Government personnel who will be involved with the TO. The meeting will provide the opportunity to discuss technical, management, and security issues, and travel authorization and reporting procedures. At a minimum, the attendees shall include Key Contractor Personnel, representatives from the Directorates, the FEDSIM Contracting Officer's Representative (COR), the Contracting Officer (CO), the Technical Point of Contact (TPOC), and other relevant Government personnel. The contractor shall provide a Kick-Off Agenda and Kick-Off Meeting Presentation **(Section F.3, Deliverables 02 and 03)** that shall provide, at a minimum, the following type of information:

1. Introduction of team members and personnel
   a. Roles and Responsibilities, including staffing plan and project organization
   b. Overview of the contractor organization to support varying locations of work
2. Communication Plan/Lines of Communication overview (between the contractor and Government)
3. Approach to reaching proposed staffing levels to allow for operational support for time constraint occurrences identified in Section C.4.1.9, Transition-In Plan

4. TO Management
    a. Overview/outline of the Project Management Plan (PMP)
    b. Overview of project tasks
    c. Overview of the Quality Control Plan (QCP)
    d. TO logistics
5. TO Administration
    a. Review of Government-Furnished Information (GFI) and Government-Furnished Equipment (GFE)
    b. Invoice review and submission procedures
    c. Travel notification and processes
    d. Security requirements/issues/facility/network access procedures
    e. Sensitivity and protection of information.
    f. Reporting requirements, e.g., Monthly Status Report (MSR)
6. Additional administrative items

The contractor shall draft and provide a Kick-Off Meeting Report **(Section F.3, Deliverable 04)** IAW Section C.4.1.7, Prepare Meeting Reports, documenting the Kick-Off Meeting Discussion and capturing any action items.

C.4.1.2 SUBTASK 1.2 – PREPARE A MONTHLY STATUS REPORT (MSR)

The contractor shall develop and provide an MSR **(Section F.3, Deliverable 05)** using Microsoft (MS) Office Suite applications, by the tenth of each month via electronic mail to the TPOC and the FEDSIM COR. The MSR shall include the following:

1. Activities during reporting period, by task (include: on-going activities, new activities, activities completed; progress to date on all above mentioned activities). Start each section with a brief description of the task.
2. Problems and corrective actions taken. Also include issues or concerns and proposed resolutions to address them.
3. Personnel gains, losses, and status (security clearance, etc.)
4. Government actions required
5. Summary of trips taken, conferences attended, etc. (attach Trip Reports to the MSR for reporting period)
6. Accumulated invoiced cost for each CLIN up to the previous month
7. Projected cost of each CLIN for the current month

The MSR shall be prepared IAW the sample provided in **Section J, Attachment C**.

C.4.1.3 SUBTASK 1.3 – CONVENE TECHNICAL STATUS MEETINGS

The contractor PM shall convene a monthly Technical Status Meeting with the TPOC, FEDSIM COR, and other Government stakeholders. The purpose of this meeting is to ensure all stakeholders are informed of the monthly activities and the MSR, provide opportunities to identify other activities and establish priorities, and coordinate resolution of identified problems or opportunities. The contractor PM shall provide minutes of these meetings, including

attendance, issues discussed, decisions made, and action items assigned, to the FEDSIM COR within five workdays following the meeting **(Section F.3, Deliverable 10)**.

C.4.1.4 SUBTASK 1.4 – PREPARE A PROJECT MANAGEMENT PLAN (PMP)

The contractor shall document all support requirements in a PMP. The contractor shall prepare and deliver a Final PMP **(Section F.3, Deliverable 07)**.

The PMP shall contain at a minimum the following:

1. Describe the proposed management approach
2. Contain detailed Standard Operating Procedures (SOPs) for all tasks
3. Include milestones, tasks, and subtasks required in this TO
4. Provide for an overall Work Breakdown Structure (WBS) and associated responsibilities and partnerships between Government organizations
5. Include the contractor's QCP

The contractor shall provide the Government with a draft PMP **(Section F.3, Deliverable 06)** on which the Government will make comments. The final PMP shall incorporate the Government's comments.

C.4.1.5 SUBTASK 1.5 – UPDATE THE PROJECT MANAGEMENT PLAN (PMP)

The PMP is an evolutionary document that shall be updated annually at a minimum **(Section F.3, Deliverable 08)**. The contractor shall work from the latest Government-approved version of the PMP.

C.4.1.6 SUBTASK 1.6 – PREPARE TRIP REPORTS

The contractor shall submit a Trip Report(s) **(Section F.3, Deliverable 09)**, as requested by the TPOC and/or FEDSIM COR. The contractor shall submit Trip Reports three working days after completion of a trip for all long-distance travel. The Trip Report shall include the following information:

1. Personnel traveled
2. Dates of travel
3. Destination(s)
4. Purpose of trip
5. Summarized cost of the trip
6. Approval authority
7. Summary of action items and deliverables

The contractor shall keep a historical summary/spreadsheet of all long-distance travel, to include, at a minimum, the name of the employee, location of travel, duration of trip, and trip estimate.

C.4.1.7 SUBTASK 1.7 – PREPARE MEETING REPORTS

The contractor shall prepare and submit Meeting Reports **(Section F.3, Deliverable 10)** as requested by the TPOC and/or FEDSIM COR, to document results of meetings. The Meeting Report shall include the following information:

1. Meeting attendees and their contact information – at minimum identify organizations represented
2. Meeting dates
3. Meeting location
4. Meeting agenda
5. Purpose of meeting
6. Summary of events (issues discussed, decisions made, and action items assigned)

C.4.1.8 SUBTASK 1.8 –QUALITY CONTROL PLAN (QCP)

The contractor shall prepare a **QCP (Section F.5, Deliverable 11)** identifying its approach to ensure quality control in meeting the requirements of each Task Area of the TO (i.e., not just the corporate generic quality control process). The contractor shall describe its quality control methodology and approach for determining and meeting performance measures identified.

The QCP shall contain at a minimum the following:

1. Performance Monitoring Methods
2. Performance Measures
3. Approach to ensure that cost, performance, and schedule comply with task planning
4. Methodology for continuous improvement of processes and procedures
5. Government Roles
6. Contractor Roles

The contractor shall provide a final QCP that incorporates the Government's comments **(Section F.3, Deliverable 12)**. The contractor shall periodically update the QCP, as required in Section F, as changes in program processes are identified **(Section F.3, Deliverable 13).**

C.4.1.9 SUBTASK 1.9 – TRANSITION-IN

The contractor shall ensure that there will be minimum service disruption to vital Government business and no service degradation during and after transition. All transition activities will be completed within 90 days after approval of final Transition Plan **(Section F.3, Deliverable 15)**. The contractor shall update the proposed Transition-In Plan **(Section F.3, Deliverable 14)**, submitted with the contractor's proposal, as appropriate, within five workdays of project start.

For the purposes of this TO, staffing is defined as the submission of current, accurate, and complete Security In-Process (SIP) forms on individuals with an active Top Secret (TS) Clearance with Sensitive Compartmented Information (SCI) eligibility (within scope – five years) and a current adjudicated Counter-Intelligence (CI) polygraph (within scope – seven years at the discretion of the government) to the USCYBERCOM Staff Security Office (SSO). If inaccuracies are identified, the forms will be rejected by the USCYBERCOM SSO and resubmission may be required. The Government will not be held responsible for inaccurate or inconsistent SIP forms that delay staffing. For tracking purposes, the FEDSIM COR shall be copied on all final or updated SIP form submissions to the USCYBERCOM SSO. The Transition-In Plan shall describe a solution for attaining the following minimum staffing levels:

1. All TO Positions: All TO requirements require 50 percent staffing at project start and 100 percent staffing within 60 days. The apportionment of the appropriate staff, until

reaching full staffing level at 100 percent, shall be coordinated with, and approved by, the FEDSIM COR. Staffing is defined as submitting a complete, accurate security package to USCYBERCOM, as stated above.

2. During the transition-in period, the contractor shall prepare to meet all TO requirements and ensure all incoming personnel are trained and qualified to perform no later than (NLT) the full performance start date.
3. During the transition-in period, the contractor's personnel shall interface with Government personnel and other contractor personnel for purposes of transferring knowledge, lessons learned, and continuity of information and documents for the commencement of performance.
4. When optional support services are executed, the requirements require 50 percent staffing upon receipt of funding and 100 percent staffing within 60 days. The apportionment of the appropriate staff, until reaching full staffing level at 100 percent, shall be coordinated with, and approved by, the FEDSIM COR.
5. The contractor shall respond to providing surge support in response to identified crisis action matters with the urgency the matter entails. Surge support may be required to be staffed and worked within USCYBERCOM spaces, following the first notification informing the contractor of a request for surge support.

All facilities, equipment, and materials to be utilized by the contractor personnel during performance of the TO after the full performance start date will be accessible to contractor personnel during the transition-in period. The contractor shall implement its Transition-In Plan when the Government accepts the Plan as final.

C.4.1.10 SUBTASK 1.10 – TRANSITION-OUT

The Transition-Out Plan shall facilitate the accomplishment of a seamless transition from the incumbent to an incoming contractor/Government personnel at the expiration of the TO. The contractor shall provide a Transition-Out Plan **(Section F.3, Deliverable 16)** NLT 90 calendar days prior to expiration of the TO. The contractor shall identify how it will coordinate with the incoming contractor and/or Government personnel to transfer knowledge regarding the following:

1. Project management processes
2. Points of contact
3. Location of technical and project management documentation
4. Status of ongoing technical initiatives
5. Appropriate contractor to contractor coordination to ensure a seamless transition
6. Transition of Key Personnel
7. Schedules and milestones
8. Actions required of the Government

The contractor shall also establish and maintain effective communication with the incoming contractor/Government personnel for the period of the transition via weekly status meetings.

The contractor shall implement its Transition-Out Plan NLT 90 calendar days prior to expiration of the TO. All facilities, equipment, and material utilized by the contractor personnel during

performance of the TO shall remain accessible to the contractor personnel during the transition-out period pursuant to the applicable security in-processing and out-processing guidelines.

C.4.1.11 SUBTASK 1.11 - ACCOUNTING FOR CONTRACT SERVICES

The Office of the Assistant Secretary of the Army (Manpower & Reserve Affairs) operates and maintains a secure Army data collections site where the contractor shall report ALL contractor manpower (including subcontractor manpower) required for performance of this contract. The contractor is required to completely fill in all the information in the format using the following web address: https://cmra.army.mil. The required information includes:

a. Contracting Office, CO, COR.
b. Contract number, including Task and Delivery Order number.
c. Beginning and ending dates covered by reporting period.
d. Contractor name, address, phone number, and email address, and identity of contractor employee entering data.
e. Estimated direct labor hours (including subcontractors).
f. Estimated direct labor dollars paid this reporting period (including subcontractors).
g. Total payments (including subcontractors).
h. Predominant Federal Service Code (FSC) reflecting services provided by the contractor (separate predominant FSC for each subcontractor if different).
i. Estimated data collection costs.
j. Organizational title associated with the Unit Identification Code (UIC) for the Army Requiring Activity (the Army requiring Activity is responsible for providing the contractor with its UIC for the purposes of reporting this information).
k. Locations where contractor and subcontractor perform the work (specified by zip code in the United States (U.S.) and nearest city and country (when in overseas locations), using standardized nomenclature on website).
l. Presence of deployment or contingency contract language.
m. Number of contractor and subcontractor employees deployed in theater this reporting period (by country).

As part of its submission, the contractor shall also provide the estimated total cost (if any) incurred to comply with this reporting requirement. Reporting period will be the period of performance, NTE 12 months ending September 30 of each Government fiscal year and must be reported by October 31 of each calendar year or at the end of the contract, whichever comes first. Contractors may use Extensible Markup Language (XML) data transfer to the database server or fill in the fields on the website. The XML direct transfer is a format for transferring files from a contractor's systems to the secure web site without the need for separate data entries for each required data element at the website. The specific formats for the XML direct transfer may be downloaded from the web.

C.4.2 TASK 2 – PROVIDE CYBERSPACE OPERATIONS SUPPORT

The contractor shall provide Cyberspace Operations support. Cyberspace Operations support includes operational requirements development, gap analysis activities, orders development

process, operations assessment process, and critical technical research and analysis as described in one through six below and apply to all subtasks of Task 2:

1. Operational Requirements Development

The contractor shall assist in identifying requirements and making recommendations for the prioritization of requirements for development. The contractor shall support USCYBERCOM's requirements process through facilitation of and participation in requirement boards and working group activities.

2. Gap Analysis Activities

The contractor shall support gap analysis activities by comparing, documenting, and reporting shortfalls in proposed cyber capabilities. The contractor shall assess how well the capability meets the requirements and intent of the development objective, document any gaps that may exist, and assess the alignment of the capability with DoD policies. The contractor shall provide written documentation to address areas of concern for shortfalls and recommended COAs **(Section F.3, Deliverable 20)**.

3. Operations Orders Process

USCYBERCOM J3 is responsible for the USCYBERCOM orders development process, as well as ensuring plans and orders are feasible, acceptable, and compliant with USCYBERCOM guidance and doctrine. J3 facilitates the transition of plans to orders by developing, implementing, and managing the operational orders process.

The contractor shall perform the following operations orders process support:

a. Develop, coordinate, and maintain USCYBERCOM orders IAW with USCYBERCOM Instruction 3300-09
b. Develop, coordinate, and maintain USCYBERCOM directives
c. Coordinate and collaborate on draft orders and directives from external partners, as required
d. Gather and prepare supporting documentation, coordinate drafts, obtain approval, and provide the final documents for publishing
e. Update orders and directives based upon evolving cyberspace environments
f. Advise USCYBERCOM leadership on all aspects of orders processing

4. Operational Assessment Process

The operational assessments process feeds the USCYBERCOM Commander's decision cycle, helping to determine the results of tactical actions in the context of overall mission objectives and providing potential recommendations for the refinement of future plans. Operational assessments provide the Commander with the current state of the operational environment, the progress of the campaign or operation, and recommendations to account for discrepancies between the actual and predicted progress. The contractor shall provide expertise in Operations Research/System Analysis (ORSA) and/or mathematics/statistics.

The contractor shall perform the following operations assessment process support:

a. Develop, analyze, and update metrics to assess J3 operational performance and effectiveness
b. Incorporate metrics into a strategic assessment process
c. Maintain a repository of Measures of Performance (MOPs) and Measures of Effectiveness (MOEs) metric results
d. Continuously monitor and provide updates to a current situation within the construct of an operation and the progress of that operation
e. Evaluate an operation against MOEs and MOPs to determine progress relative to the mission objectives and end states
f. Develop recommendations and guidance for improvement in the operation to help drive the Commander's decision cycle

5. Critical Technical Research and Analysis

The contractor shall conduct critical and technical research and analysis and assist efforts to define Commander's Critical Information Requirements (CCIR), Priority Intelligence Requirements (PIR), and Essential Elements of Friendly Information (EEFI) for reporting cybersecurity incidents **(Section F.3, Deliverable 20)**.

6. Executive Summaries

The contractor shall develop one page, topically and technically accurate, executive summaries that summarize specific operations efforts for senior leaders.

C.4.2.1 SUBTASK 2.1 – PROVIDE DODIN OPERATIONS SUPPORT

DODIN Operations conducts global, operational planning to secure, operate and defend the DODIN and its critical dependencies IOT provide full spectrum Cyberspace Operations ensuring freedom of maneuver in that domain and denying our adversaries the same. The contractor shall provide expertise in DODIN Operations, cyber defense, Tactics, Techniques, and Procedures (TTP) and systems, Cyberspace Operations community architecture, current and emerging cyber threats, and potential offensive and defensive capabilities for countering cyber threats. Additionally, the contractor shall provide expertise in electronic communications concepts to include the systems development life cycle, equipment specifications, network management, and analytical techniques.

The contractor shall provide the following DODIN Operations support:

1. Assess boundary protection statistics as provided by the Defense Information Systems Agency (DISA) and/or other organizations, and determine readiness of the DODIN and contribute input to reports for USCYBERCOM leadership **(Section F.3, Deliverable 20)**
2. Publicize the current defense policy to the DoD community and evaluate requests for boundary defense policy changes or exceptions from applicable staff elements, Joint Forces Headquarters (JFHQs), subordinate headquarters, Service Cyber components, Combatant Command (CCMD), and components and agencies with cyber-related missions

3. Conduct research and produce, white papers **(Section F.3, Deliverable 19)**, reports **(Section F.3, Deliverable 17)**, and presentations that focus on rapidly emerging cyber threats and cyber adversary TTP
4. Conduct proof of concept development of cyber capabilities for countering ongoing or impending cyber adversary actions against United States (U.S.) Government networks
5. Recommend TTPs for countering cyber threats

C.4.2.1.1 SUBTASK 2.1.1 – PROVIDE INFORMATION NETWORK DEFENSE SUPPORT

Information network defense is responsible for identifying and integrating network defense requirements into DoD programs and projects that execute the "operate and defend" aspect of USCYBERCOM's mission. The contractor shall provide telecommunications, networking, and DoD network design expertise.

The contractor shall provide the following information network defense support:

1. Monitor testing of systems, plan and direct Rehearsal of Concept (ROC) drills in coordination with DISA and applicable USCYBERCOM staff elements, JFHQs, subordinate headquarters, Service Cyber components, CCMD, and components and agencies with cyber-related missions (as required) in efforts to validate operational procedures throughout the development of new defensive tools, from before Initial Operational Capability (IOC) to Full Operational Capability (FOC)
2. Coordinate with applicable USCYBERCOM staff elements, JFHQs, subordinate headquarters, Service Cyber components, CCMD, and components and agencies with cyber-related missions to identify, assess, and develop effective options for cyberspace defense strategies
3. Support DCO planning, CONOPS development, and mission execution through expert knowledge of USCYBERCOM components, infrastructure, processes, capabilities, authorities, and partner operations
4. Provide expert information and recommendations to applicable USCYBERCOM staff elements, JFHQs, subordinate headquarters, Service Cyber components, CCMD, and components and agencies with cyber-related missions to support implementation of strategies and plans
5. Coordinate and collaborate with partners and stakeholders to ensure seamless integration of services, systems, and networks into existing and future joint DODIN infrastructure
6. Coordinate with applicable USCYBERCOM staff elements, JFHQs, subordinate headquarters, Service Cyber components, CCMD, and components and agencies with cyber-related missions to identify, assess, develop, and codify across the enterprise a common Cyber Key Terrain (CKT) Program
7. Conduct research and produce white papers **(Section F.3, Deliverable 19)**, reports **(Section F.3, Deliverable 17)**, and presentations that focus on rapidly emerging cyber threats and cyber adversary TTP

C.4.2.1.2 SUBTASK 2.1.2 – PROVIDE PLATFORM INFORMATION TECHNOLOGY-CONTROL SYSTEMS (PIT-CS) SUPPORT

USCYBERCOM coordinates securing and defending DoD-owned PIT-CS as required to keep the operational environment safe, secure, and resilient against current and emerging cyber threats. The contractor shall provide expertise in PIT-CS cybersecurity threats and vulnerabilities and current safeguards for PIT-CS.

The contractor shall provide the following PIT-CS support:

1. Develop guidance on PIT-CS incident prevention, information, and analysis
2. Develop input to organizational policies and procedures related to PIT-CS incident response
3. Analyze the operational impacts of PIT-CS incidents, coordinate, and provide the information to the applicable DoD organization
4. Create and participate in test PIT-CS incident response plans
5. Participate, assist, and advise various Operational Planning Groups (OPGs) and Operational Planning Teams (OPTs) by providing functional expertise and guidance on PIT-CS incidents
6. Develop after action reports **(Section F.3, Deliverable 18)** for post-PIT-CS assessment and incident response activities
7. Gather forensic information to support PIT-CS incident analysis
8. Recommend safeguards to prevent PIT-CS intrusions
9. Remediate PIT-CS after an incident
10. Conduct research and produce, white papers **(Section F.3, Deliverable 19)**, reports **(Section F.3, Deliverable 17)**, and presentations that focus on rapidly emerging cyber threats and cyber adversary TTP

C.4.2.1.3 SUBTASK 2.1.3 – PROVIDE MOBILE DEFENSE OPERATIONS SUPPORT

The USCYBERCOM J3 must understand the threat from mobile devices that house distributed sensitive data storage and access mechanisms, lack consistent patch management and firmware updates, and have a high probability of being hacked, lost, or stolen. Mobile phones and tablets have become critical systems for a wide variety of production applications from Enterprise Resource Planning (ERP) to project management. The contractor shall provide expertise in mobile hardware and software (hands-on experience), security tools for mobile systems, common mobile exploit methods, and wireless network analysis tools for identifying and exploiting wireless networks used by mobile devices.

The contractor shall provide the following mobile defense operations support:

1. Conduct analysis of post-forensic reports and research of compromised mobile devices on the DODIN and provide an analysis of and recommendations report **(Section F.3, Deliverable 20)** for mitigation and planning
2. Conduct security assessments of mobile applications and platforms and provide analysis and recommendation report (**Section F.3, Deliverable 20)**
3. Participate, assist, and advise various OPGs and OPTs by providing functional expertise and guidance on mobile devices
4. Coordinate with applicable USCYBERCOM staff elements, JFHQs, subordinate headquarters, Service Cyber components, CCMD, and components and agencies with

cyber-related missions to identify, assess, and develop effective options for mobile defense strategies

5. Conduct research and produce white papers **(Section F.3, Deliverable 19)**, reports **(Section F.3, Deliverable 17)**, and presentations that focus on rapidly emerging cyber threats and cyber adversary TTP

C.4.2.2 SUBTASK 2.2 – PROVIDE SPACE DOMAN CYBERSPACE OPERATIONS SUPPORT (OPTIONAL)

Cyberspace Operations in the space domain is performed IOT thwart attacks and risks against space-based platforms and resources that collect, process, store, disseminate, and manage information.

The contractor shall provide the following space domain Cyberspace Operation support:

1. Provide Satellite Communications (SATCOM) and space-related deliberate and planning support for Cyberspace Operations
2. Provide Positioning, Navigation, and Timing (PNT), SATCOM, and other Space Force Enhancement (SFE) capability planning support for DCO
3. Support working groups to define Cyberspace Operations and planning requirements, synchronization of resources, and prioritization of sustainment issues between the cyberspace and space domains
4. Coordinate with partners and stakeholders to define strategies, policies, plans, and procedures to affect the holistic planning and management of the DODIN and JIE from existing to future SFE, Global Positioning System (GPS), and SATCOM system configurations in a manner transparent to customers and ongoing operations
5. Provide GPS and SATCOM system-level planning support for Cyberspace Operations
6. Conduct research and produce reports **(Section F.3, Deliverable 17)** and presentations that focus on rapidly emerging cyber threats and cyber adversary TTP

C.4.2.3 SUBTASK 2.3 – PROVIDE INTERNATIONAL/NATIONAL CYBERSPACE OPERATIONS SUPPORT

The USCYBERCOM J3 conducts activities ISO the various CCMDs, including strengthening relationships with key partner nations, coordinating, synchronizing, deconflicting, and integrating operational planning efforts for Cyberspace Operations. This task will require the contractor to maintain a broad, expert knowledge of the Command's cyber missions, authorities, and capabilities as well as equivalent information regarding the roles and responsibilities of the Command's external program partners, which includes (but is not limited to) other DoD commands and agencies, other U.S. Government agencies and key partners.

The contractor shall provide the following international/national Cyberspace Operations support:

1. Communicate complex programmatic cyber planning information, orally and in writing, to elicit understanding and support from professional peers and non-specialists
2. Contribute to the development and refinement of COAs and other cyber guidance materials utilized by the Command and its external cyber program partners

3. Evaluate national/international operations and recommend opportunities for USCYBERCOM to execute authorities to meet DoD cyber objectives
4. Provide expert information and recommendations to applicable USCYBERCOM staff elements, JFHQs, subordinate headquarters, Service Cyber components, CCMD, and components and agencies with cyber-related missions to support implementation of strategies and plans
5. Assist and advise various OPGs and OPTs by providing functional expertise and guidance as to the intent of negotiated and established national/international agreements
6. Participate in post-event analyses to determine the success of cyber strategies, initiatives, or plans
7. Attend strategic working group meetings, facilitate discussions, gather information, analyze the data, and produce written products ISO USCYBERCOM's force management efforts
8. Review and provide feedback on cyber-related strategy, policy, and doctrine received from higher headquarter(s)
9. Report on evolving cyberspace policy trends and issues within the U.S. Government
10. Review and evaluate cyberspace policy directives and CONOPS
11. Assist with responses to Congressionally Directed Actions (CDA) and Congressional Questions for the Record (QFR)
12. Provide input to the Joint Quarterly Readiness Review (JQRR) submission for USCYBERCOM
13. Provide support with technical and policy analyses of cyber issues
14. Attend conferences, seminars, and special meetings as identified by the Government
15. Contribute to the Office of the Secretary of Defense (OSD) and U.S. Strategic Command (USSTRATCOM)/USCYBERCOM policies and directives on cybersecurity and internet access
16. Provide substantive input in converting cybersecurity policies into operational plans for defense of the DODIN, as well as maintain a set of detailed options and filtering/defense policies for expected DODIN Operations and defense scenarios, attacks, and changes in DODIN defensive posture
17. Assist in advocating USCYBERCOM cyberspace policy and doctrine within the DoD and across the U.S. Government through the Joint Interagency Coordination Group (JIACG). Provide analysis, recommendations, and guidance on cyberspace policy
18. Assist in establishing USCYBERCOM engagement through a JIACG and provide representation to policy and doctrine forums of the DoD
19. Recommend policy for the deconfliction of military Cyberspace Operations with other U.S. Government organizations, specified partners, and allies as necessary

C.4.2.4 SUBTASK 2.4 – PROVIDE JIE OPERATIONS SPONSOR GROUP (JOSG) OPERATIONS SUPPORT

The JIE effort will realign, restructure, and modernize how the DoD IT networks and systems are constructed, operated, and defended. JIE will consolidate and standardize the design and architecture of the DoD's networks to improve mission effectiveness, increase cybersecurity, and

optimize resources and IT efficiencies. USCYBERCOM leads the JOSG, which serves as the operational sponsor for the JIE. The JOSG is responsible for developing, integrating, and synchronizing operational procedures ISO the JIE initiative. The JOSG follows the direction of the JIE Planning and Coordination Cell (PCC) and updates the JIE Executive Committee through the PCC.

The contractor shall provide the following JOSG operations support:

1. Develop operational artifacts required to support delivery of JIE
2. Support the JIE Technical Synchronization Office (JTSO) in identifying gaps and overlaps across existing DODIN Operations and DCO technical capabilities
3. Assess and deconflict JIE with DODIN Operations and DCO, and provide an analysis and recommendation report **(Section F.3, Deliverable 20)** to align DODIN planning efforts with JIE
4. Assist in the development and refinement of the JIE C2 Construct and the JIE Operational CONOPs
5. Develop, integrate, and maintain operational TTPs and SOPs ISO the JIE
6. Coordinate and collaborate with JTSO and the USCYBERCOM Command, Control, Communications, Computers & Information Technology (C4IT) Directorate (J6) to ensure seamless integration of services, systems, and networks into existing and future joint DODIN infrastructure
7. Assess and recommend network management policies and procedures for implementation in JIE in coordination with JIE partners, stakeholders, and the C4IT Directorate
8. Organize, coordinate, and participate in JOSG working groups and other JIE workshop type of events
9. Develop, staff, and maintain accurate USCYBERCOM orders and directives
10. Develop and conduct update briefs, presentations, and papers to USCYBERCOM leadership to ensure situational awareness and status are conveyed related to the assigned project areas **(Section F.3, Deliverable 17)**
11. Contribute to the development and refinement of JIE documentation, to include cohesiveness of message, consistency of content, version control, and adjudication of comments.

C.4.2.4.1 SUBTASK 2.4.1 – PROVIDE JOSG REQUIREMENTS SUPPORT

The JOSG is responsible for developing the operational requirements needed to drive the implementation of JIE. The JOSG tracks the requirements from creation to implementation.

The contractor shall provide the following JOSG requirements support:

1. Coordinate with JIE stakeholders to identify JIE operational requirements
2. Develop recommended prioritization and sequencing of JIE operational capability implementation and transition
3. Ensure capabilities align with DoD governing policies and meet the intent of the development objective or capability
4. Analyze proposed capabilities, recommend COAs, and develop solutions to address areas of concern for shortfalls in JIE implementation

5. Develop processes and procedures **(Section F.3, Deliverable 21)** to implement and ensure JIE operational requirements are met DoD-wide
6. Identify DODIN Operations and DCO enterprise management tool requirements and evaluate operational standards and tools for use within JIE
7. Coordinate with JIE stakeholders to advise and assist with the planning and identification of cyber defense requirements associated with JIE operational requirements

C.4.2.4.2 SUBTASK 2.4.2 - PROVIDE JOSG OPERATIONS COMPLIANCE AND IMPLEMENTATION SUPPORT

The JOSG is responsible for shaping operational performance metrics for JIE and tracking JIE implementation and ensuring compliance with established standards.

The contractor shall provide the following JOSG operations compliance and implementation support:

1. Coordinate with the Office of the DoD Chief Information Officer (CIO) and other stakeholders to develop, distribute, and sustain operational metrics for the JIE
2. Track all DoD components' compliance with JIE MOEs/MOPs and applicable DoD JIE policies
3. Devise methods to test and evaluate each component's compliance with JIE requirements and all other applicable standards
4. Develop and maintain processes, procedures, and TTPs for the Operations Center accreditation process **(Section F.3, Deliverable 21)**
5. Develop and monitor JIE Service Level Agreement (SLA) performance and metrics
6. Provide evaluation results, reports, and recommendations **(Section F.3, Deliverable 20)** to USCYBERCOM and JIE leadership
7. Support DCO planning and mission execution through expert knowledge of USCYBERCOM components, processes, capabilities, authorities, and partner operations
8. Analyze and evaluate voice/video/data system solutions, provide an analysis and recommendation report **(Section F.3, Deliverable 20)**, and provide support for joint full spectrum (terrestrial and space) system and network integration in the JIE

C.4.2.5 SUBTASK 2.5 – PROVIDE CYBER FIRES PLANNING AND ANALYSIS SUPPORT

Cyber fires planning and analysis supports planning in OCO and DCO throughout the entire JOPP. Cyber fires planning and analysis requires the coordination of joint strategic and operational planning and execution of joint fires, to include targeting, capability pairing, and threat mitigation ISO Cyber Mission Force (CMF) and other operations. Knowledge of cyber TTPs is required IOT provide recommendations to USCYBERCOM leadership on all aspects of joint fires and threat mitigation.

The contactor shall provide the following cyber fires planning and analysis support:

1. Plan, organize, determine, and recommend necessary policies, regulations, directives, programs, doctrine, and procedures for the establishment and maintenance of assigned and anticipated joint fires coordination and execution

2. Provide support to future operations planners to integrate cyber capabilities into plans
3. Collaborate with DISA, the National Security Agency (NSA), service providers, and other organizations to ensure that USCYBERCOM requirements are implemented
4. Collaborate with operators in the Joint Operations Center (JOC), subordinate headquarters, and cyber teams to integrate capabilities
5. Coordinate with all applicable USCYBERCOM staff elements, JFHQs, subordinate headquarters, Service Cyber components, CCMD, and components and agencies with cyber-related missions
6. Act as liaison between capability Subject Matter Experts (SMEs) and the planning teams IOT assist the planners in understanding the technical aspects of specific capabilities ISO a specific planning effort
7. Identify and develop cyber TTPs that advise the future operations planners on achieving cyberspace operations ISO operations and exercise objectives
8. Recommend requirements and prioritization for the development of automated cyberspace capabilities ISO operations and assessments
9. Participate in USCYBERCOM requirements working groups as a capability SME to define cyber capabilities/tools and recommend COAs
10. Assess and provide an analysis and recommendation report **(Section F.3, Deliverable 20)** on technical issues relating to current and future DoD plans, programs, policies, and activities related to Cyberspace Operations
11. Participate in special programs and teams for fires planning and analysis
12. Support the collateral Review and Approval Process for Cyberspace Operations (RAP-CO) process.

C.4.2.5.1 SUBTASK 2.5.1 – PROVIDE CYBER TASKING CYCLE (CTC) SUPPORT

The CTC is the official method used to task cyber forces to execute missions. The CTC is utilized at all echelons of a joint command to globally synchronize and deconflict forces. The USCYBERCOM J3 is responsible for managing the products that are driven by the CTC.

The contactor shall provide the following cyber tasking cycle support:

1. Assist with the creation, implementation, and management of the Master Cyber Operations Plan (MCOP) creation and implementation
2. Synchronize and deconflict the CTO
3. Attend and provide input during the Operations Synchronization meetings
4. Coordinate with CMF and other subordinate units to facilitate the CTC processes
5. Provide time-sensitive, critical data inputs into the C2 system and validate data
6. Make recommendations on changes in the C2 system based upon evolving task cycle

C.4.2.5.2 SUBTASK 2.5.2 – PROVIDE FIRES OUTREACH AND EXERCISE PROGRAM SUPPORT

The fires outreach program provides information and knowledge to different groups, courses, units, and organizations outside of USCYBERCOM on the USCYBERCOM fires process as it

continues to evolve. This program has become even more important with the standup of the CMF units.

The contactor shall provide the following fires outreach and exercises program support:

1. Conduct outreach programs on USCYBERCOM Fires processes
2. Maintain the master Fires Brief with the most updated information
3. Represent USCYBERCOM and brief at selected courses and events **(Section F.3, Deliverable 17)**, to include, but not limited to, selected exercise academics, the Joint Advanced Cyber Warfare Course (JACWC), the Army Cyberspace Operations Course, the Air Force Weapons School, and the Joint Targeting School
4. Maintain contact with the external groups, courses, units, and organizations and provide approved, updated fires briefings and supporting documentation in a timely manner
5. Participate in exercises, including CCMD exercises and planning conferences, and provide feedback and after action reports **(Section F.3, Deliverable 18)**.

C.4.2.5.3 SUBTASK 2.5.3 – PROVIDE SPECIAL TECHNICAL OPERATIONS (STO)/SPECIAL ACCESS PROGRAM (SAP) CYBER FIRES PLANNING AND ANALYSIS SUPPORT

STO/SAP cyber fires planning and analysis entails the synchronization and deconfliction of collateral and STO/SAP capabilities within the JOPP. STO/SAP cyber fires planning and analysis requires the ability to pass an additional layer of security review and must adhere to need-to-know and material contribution criteria. The contractor shall provide expertise in Cyberspace Operations and cyber fires IOT effectively integrate with USCYBERCOM Fires and Effects.

The contactor shall provide the following STO/SAP Cyber Fires Planning and Analysis support:

1. Support the RAP-CO, assist in the development of CONOPs for employment of STO/SAP capabilities ISO USCYBERCOM supported and supporting Cyberspace Operations
2. Integrate STO/SAP capabilities in current and future operations and plans ISO USCYBERCOM and CCMDs
3. Assist with STO/SAP assessments and document findings in an analysis and recommendation report **(Section F.3, Deliverable 20)**.

C.4.2.6 SUBTASK 2.6 – PROVIDE INFORMATION ASSURANCE VULNERABILITY MANAGEMENT (IAVM) SUPPORT

The IAVM Program supports secure Cyberspace Operations through the identification and analysis of disclosed vulnerabilities to determine their operational impact to the DODIN. Vulnerabilities found to pose a significant risk to the DODIN are addressed by the IAVM Program through dissemination of IAVM Directives (Information Assurance Vulnerability Alerts (IAVA) and Information Assurance Vulnerability Bulletins (IAVB)) mandating DODIN-wide implementation of mitigation or remediation actions. The contractor shall provide expertise in computer network theory, cybersecurity standards, policies, and methods, as it applies to the lifecycle of cyberspace threats, attack vectors, and methods of exploitation.

The contractor shall provide the following IAVM support:

1. Identify and draft mitigation strategies for vulnerabilities without vendor-provided remediation for the Government's review
2. Establish communications with vendors for the incorporation of newly identified vulnerability mitigation strategies ensuring adherence to specialized and proprietary DODIN asset requirements
3. Develop and inform the mitigation/remediation strategy in response to publicly disclosed vulnerabilities of vendor software/hardware products
4. Review daily, weekly, monthly, and annual vulnerability metric roll-ups associated with affected and non-compliant DoD assets
5. Utilize risk scoring and monitoring tools/capabilities to review manually uploaded and automated information from DoD component to report vulnerability orders and directives compliance.
6. Develop, coordinate, and maintain accurate IAVM alerts and bulletins IAW the Commander Joint Chiefs of Staff Manual (CJCSM) 6510.02. Create situational awareness products to provide USCYBERCOM leadership and DoD components with detailed information related to vulnerabilities and appropriate mitigation strategies
7. Assist with the prioritization of newly identified software/hardware vulnerabilities based upon severity, potential operational impact, exploitation, and other factors to assess risk to DODIN assets
8. Analyze known issues affecting DoD components with vendor-provided fixes and liaise with the appropriate vendor for a defined and attainable solution
9. Collaborate and coordinate with JFHQ's, DoD Combatant Commands/Services/Agencies/Field Activities (CC/S/A/FA), Intelligence Agencies, Law Enforcement (LE), and U.S. Government organizations
10. Develop, document, and convey IAVM operational requirements to enhance capabilities identifying, tracking, and remediating system and network vulnerabilities as well as automated vulnerability management capabilities
11. Monitor the progress of and collaborate with internal and external organizations to ensure IAVM operational requirements and strategies are fulfilled and adhered
12. Consolidate, analyze, and brief reports **(Section F.3, Deliverable 17)** on new and existing adversary TTPs

C.4.2.6.1 SUBTASK 2.6.1 – PROVIDE INFORMATION ASSURANCE VULNERABILITY ALERTS (IAVA) COMPLIANCE SUPPORT

IAVA directives address recently disclosed vulnerabilities that introduce immediate and severe risk to DODIN assets. Corrective actions are mandatory due to the severity of the vulnerability. USCYBERCOM directs mitigations strategies for enterprise vulnerabilities through orders, directives, and policies. The contractor shall provide expertise on IAVM Program process and methods, automated cybersecurity capabilities, including Host Based Security System (HBSS), Assured Compliance Assessment Solution (ACAS), Continuous Monitoring Risk Score (CMRS), and the USCYBERCOM IAVM System.

The contractor shall provide the following IAVA compliance support:

1. Track compliance of USCYBERCOM orders and directives for implementation of appropriate security controls against DODIN assets
2. Communicate (written and oral) with JFHQs and CC/S/A/FAs concerning IAVA strategy compliance, and review and track Plan of Action and Milestones (POA&M) approval and documentation, implementation of appropriate system security controls, and DoD policies
3. Provide status reports and metrics to USCYBERCOM leadership for DoD Components on IAVA compliance
4. Review daily, weekly, monthly, and annual compliance metrics roll-ups to support USCYBERCOM operational deadlines
5. Review monthly POA&M audits on selected IAVA orders and directives to validate DoD components compliance status
6. Develop and provide programmatic review for IAVA POA&M audits, non-compliant assets, and incidents resulting from unmitigated vulnerabilities
7. Maintain the IAVM oversight program, associated policies, and provide strategic guidance for DoD component implementation
8. Conduct trend analysis of incidents to determine compliance with USCYBERCOM orders and directives
9. Collaborate with JFHQ's regarding supporting organizations' unacceptable DODIN ratings, inspection failures, and incidents to develop briefs, watch lists, and responses to requests for information
10. Maintain situational awareness of IAVA strategy programmatic issues and brief the quarterly IAVA compliance watch list **(Section F.3, Deliverable 17)**

C.4.2.7 SUBTASK 2.7 – PROVIDE COMMAND CYBER READINESS INSPECTION (CCRI) COMPLIANCE SUPPORT (OPTIONAL)

The CCRI Program is a rigorous inspection-oriented process designed to validate security compliance across the DODIN. The intent of the inspection program is to establish a framework to enforce security control compliance for DoD components and senior command accountability. This process is accomplished by utilizing the following capabilities to determine risks of non-compliance assets: Network Infrastructure (e.g., Network Intrusion Detection System (NIDS), Host Intrusion Detection System (HIDS), routers, switches, and firewalls), Network Vulnerability Scanning (e.g., vulnerability patching, Domain Name System (DNS), traditional security such as physical security), HBSS, continuous monitoring, Cross Domain Solutions (CDS), releasable networks, and wireless technologies. The contractor shall provide expertise of DCO mitigation and remediation strategies related to CCRI deficiencies, emerging threats, vulnerabilities, and inspection findings, and maintain situational awareness of threat activity directed toward DoD Components, Cleared Defense Contractors (CDCs), and non-DoD Federal Organizations.

The contractor shall provide the following CCRI compliance support:

1. Review and maintain situational awareness of CCRI inspection results and mitigation status to include identification of key issues and priorities affecting the defense of the DODIN

2. Provide USCYBERCOM guidance to JFHQs for DCO mitigation and remediation strategies related to CCRI deficiencies, emerging threats, vulnerabilities, and inspection findings
3. Acquire threat and vulnerability trend data for inspected sites and it geographical Areas of Responsibility (AORs) to determine mitigation and remediation strategies
4. Develop and disseminate mitigation/remediation guidance and methods for site inspections
5. Participate in technical working groups and discussions to influence recommendations within the CCRI strategy
6. Analyze threat and vulnerability reports from subordinate JFHQs and develop recommended strategies to significantly improve the readiness and defensive posture of the DODIN
7. Identify systemic causes of inspection/assessment failures and develop recommended courses of corrective actions to increase defensive posture of the DODIN
8. Provide programmatic support and oversight to the CCRI process by reviewing CCRI methods, reporting processes, and USCYBERCOM Threat Mitigation Framework (TMF)
9. Provide input to the development of DoD and USCYBERCOM policies, processes, procedures and operations **(Section F.3, Deliverable 21)**. Possess and maintain cognizance of national-level cyber security policies, plans, processes, and coordination procedures
10. Establish and maintain working relationship with the Intelligence, LE, and Homeland Defense Communities
11. Develop an analysis and recommendation report (**Section F.3, Deliverable 20)** on technical issues of current and future DoD plans, programs, policies, and activity related to the assessment of the DODIN
12. Identify shortfalls and capability gaps in DoD, USCYBERCOM, Defense Security Service (DSS), and Department of Homeland Security (DHS) policies and guidance
13. Analyze strategic plans and policies; and provide an analysis and recommendation report **(Section F.3, Deliverable 20)**; analysis shall be specific to DoD but include familiarity with National Industrial Security Program (NISP) and National Institute of Standards and Technology (NIST) cybersecurity requirements and leverage industry and/or academia methods for addressing current and emerging cyberspace requirements
14. Provide expertise in the development of current DODIN plans and policies supporting cybersecurity assessments, to include emerging technologies
15. Assist the Government in providing collaborative mission support with the Joint Staff, NSA, DISA, Services, and other DoD components deemed essential working groups in assessing, prioritizing and developing guidance for the DoD-wide implementation plans for the cybersecurity strategy
16. Develop white papers **(Section F.3, Deliverable 19)**, briefs, and programmatic oversight reports **(Section F.3, Deliverable 17)**.

C.4.2.8 SUBTASK 2.8 – PROVIDE FUSION SUPPORT

Fusion is the collaboration, correlation, and analysis of cyberspace incident reports derived from reliable sources, network sensors, vulnerability management devices, open source information, and DoD component-provided situational awareness of known adversary activities.

Threat detection analysis and coordination provides monitoring, correlation, and prevention of cyber threat activity targeting the DODIN. The contractor shall provide expertise on the utilization of Government and industry capabilities, best security practices, advanced log analysis, forensics, network monitoring, network flow analysis, packet capture analysis, network proxies, firewalls, and anti-virus capabilities. The contractor shall provide expertise in forensics analysis to determine adversary methods of exploiting information system security controls, the use of malicious logic, and the lifecycle of network threats and attack vectors.

The contractor shall provide the following fusion support:

1. Analyze the details of Named Areas of Interest (NAI) and advanced persistent threats that impact the DODIN, and track, correlate, harvest, trend, and report on the unique TTPs utilized
2. Conduct incident handling/triage, network analysis and threat detection, trend analysis, metric development, and security vulnerability information dissemination
3. Configure, maintain, and utilize USCYBERCOM and CC/S/A/FA capabilities IOT detect, monitor, track, and analyze malicious activity targeting the DODIN
4. Consume, review, correlate, and report on high priority DoD, Intelligence, and U.S. Government operational reporting of threats and vulnerabilities to correlate similar incidents/events, malicious tradecraft, TTPs of malicious activity, and indicators utilized to impact or target the DODIN
5. Develop consolidated notifications and updates to the USCYBERCOM JOC on threat and vulnerability activity
6. Develop, obtain Government approval of, and release situational awareness reports/products, operational directives/orders/messages, and quarterly threat analysis reports/metrics
7. Review, analyze, and maintain the content of a DoD indicator database to aid in the detection and mitigation of threat activity
8. Update DoD shared situational awareness mechanisms, including USCYBERCOM websites, Wikipedia-style solutions, and collaboration/chat mechanisms
9. Develop and present cyber threat briefings, presentations, and papers to USCYBERCOM leadership to ensure situational awareness and status are conveyed related to the assigned project areas **(Section F.3, Deliverable 17)**
10. Assist the Government by operating as the DoD community leader for the discovery of threat activity and associated indicators
11. Determine sophistication, priority, and threat level of identified malware and intrusion related TTPs
12. Develop metrics and trending/analysis reports of malicious activity used to compromise the DODIN

13. Develop, staff, and release analysis findings in technical analysis reports to the DoD Community
14. Manage a DoD prioritization process to identify priority threats and vulnerabilities that impact the DODIN
15. Develop signatures for use within DoD threat detection capabilities to detect potentially malicious activity on the DODIN
16. Coordinate with USCYBERCOM partner organizations to receive, distribute, and conduct analysis on vulnerability and threat information that impacts the DODIN and the Defense Industrial Base (DIB)
17. Assess vulnerability of DODIN Operations ISO DCO and provide an analysis and recommendation report **(Section F.3, Deliverable 20)**
18. Draft and propose USCYBERCOM guidance, directives, and products
19. Maintain situational awareness of Intrusion Problem Sets, including NAI for collaboration with the DoD cyberspace analysts and cyberspace partners
20. Develop, review, and report on DCO and cybersecurity products
21. Develop, review, and comment on incident handling procedures and reporting **(Section F.3, Deliverable 21)**
22. Coordinate analysis projects related to Intrusion Sets and NAI compromises
23. Assist in developing processes and procedures designed to facilitate increased awareness, intelligence, and technical data fusion support
24. Provide recommended improvements on cybersecurity posture through technical research and analysis
25. Provide technical research and analysis of computer forensic evidence
26. Provide recommendations to aid USCYBERCOM in assessment reporting and mitigation strategies
27. Analyze cybersecurity/DCO activities on Government systems and make recommendations for actions to protect the DODIN
28. Evaluate operational information, intelligence information, assessments and reports, Computer Emergency Readiness Team (CERT), LE/CI, allied/coalition, and open-source information to assess potential impacts on the DODIN, and provide an analysis and recommendation report **(Section F.3, Deliverable 20)**
29. Develop and propose processes and procedures designed to facilitate all-source intelligence analysis of the foreign threat picture

C.4.2.9 SUBTASK 2.9 – PROVIDE MEDIA, MALWARE, AND ANALYSIS (MMA) SUPPORT

MMA is the forensic analysis of media and software reverse engineering. The analysis consists of reviewing the contents of a compromised system, documenting unusual files and data, and identifying the TTPs used by an adversary to gain unauthorized access to DODIN assets. This includes detailed technical work on media analysis and exploitation of data from compromised systems ISO ongoing analysis.

The contractor shall provide expertise in computer network theory, communication methods and malicious properties, ethical hacking, and TTPs of advanced persistent threats.

The contractor shall provide the following MMA support:

1. Perform malware analysis and incident handling
2. Draft and implement security incident response policies
3. Analyze malware discovered in DoD intrusions; perform dynamic and static analysis and reverse engineering of intrusion artifacts
4. Develop and release Government-approved analysis findings in technical analysis reports
5. Identify unique indicators, TTPs, patterns, or heuristics from malware artifacts for the development of detection and mitigation strategies
6. Collaborate with anti-virus vendors for malware submissions to aid vendor anti-virus updates
7. Extract malicious files from digital media and sources
8. Identify, analyze, and document adversarial activities to gain unauthorized access to DoD systems
9. Develop an analysis and recommendation report **(Section F.3, Deliverable 20)** determining sophistication, priority, and threat of identified malware
10. Examine media and malware analysis reports and operational reporting from DoD incidents to correlate similar events, tradecraft, and TTPs of malicious activity
11. Develop metrics and trending/analysis reports of malicious activity used to compromise the DODIN
12. Develop, document, and convey operational requirements for the development, procurement, or implementation of media, malware analysis capabilities such as the Joint Malware Catalog (JMC), Joint Indicator Database (JID), Joint Incident Management System (JIMS), and Unified Cyber Analytics Portal (UCAP)
13. Develop and conduct update briefs, presentations, and papers to USCYBERCOM leadership to ensure situational awareness and status are conveyed related to the assigned project areas **(Section F.3, Deliverable 17)**
14. Conduct log and system analysis for various system and network capabilities, to include routers, Windows, and UNIX
15. Update DoD shared situational awareness mechanisms to include USCYBERCOM websites, Wikipedia-style solutions, and collaboration/chat mechanisms
16. Identify new exploits and security vulnerabilities, analyze behavior of malicious code, research open source data, document host/network signatures, and develop mitigation and remediation strategies
17. Provide Message Digest 5 (MD5) Hash updates. Validate, update, post, and maintain MD5 Hash list for signature repository
18. Conduct analysis on the lifecycle of adversary anatomy of attack and exploitation and the associated tools, malware, and encryption mechanisms utilized
19. Identify patterns in reported compromises and identify additional compromises as part of the same incident

C.4.2.10 SUBTASK 2.10 – PROVIDE JOINT ADVANCED TARGETING ANALYSIS SUPPORT

Joint Advanced Targeting Analysis (Fires) identifies gaps with pairing capabilities against targets to achieve an effect IAW tactical objectives, operational goals, and strategic end-states. Targeting Analysis involves collaboration and coordination of USCYBERCOM targets with the Intelligence Community (IC) and DoD Components. The contractor shall provide technical targeting expertise on the best methods to allocate fires against deliberate and dynamic targets in and through cyberspace.

The contractor shall provide the following joint advanced targeting analysis support:

1. Coordinate targeting strategy development and engagement responsibilities with components and supporting commands. Provide input to USCYBERCOM on the approval process for targeting and fires
2. Assist in the development of USCYBERCOM joint targeting policies and procedures **(Section F.3, Deliverable 21)**
3. Facilitate preparation of the Joint Targeting Working Group (JTWG) and the Joint Targeting Coordination Board (JTCB)
4. Actively participate in targeting Boards, Bureaus, Centers, Cells and Working Groups (B2C2WGs) such as the JTWGs inside and outside the Command to prioritize target requirements
5. Assist with all aspects of preparing strike packages and cyber request and approval packages to validate targets via the JTCB
6. Assist in the synchronization and implementation and prioritization of targeting methodologies
7. Monitor and facilitate all targeting list at the intermediate level and above
8. Draft Commander's targeting guidance
9. Provide input to the cyber joint targeting cycle to include interagency planning, joint targeting board support, cyber weapons capability analysis, collateral effects estimate, and planning support
10. Identify desired effects, methods of engagements, target aim points, and cyber forces in which to deliver fires or effects against military targets in and through cyberspace
11. Facilitate the stand-up and transition of fires tasks to the CMF tactical level headquarters

C.4.2.11 SUBTASK 2.11 – PERFORM CYBER CAPABILITY ANALYSIS

Cyber capability analysis develops and coordinates operational and technical requirements for enhancing cyberspace capabilities based on operational needs throughout the entire lifecycle. This process requires coordination of a time-phased implementation of capabilities to align with USCYBERCOM and CMF strategic orders and directives. Cyber capability analysis identifies, prioritizes, and develops capability requirements.

The contractor shall provide the following cyber capability analysis support:

1. Facilitate, coordinate, and assist in the development, review, and edit of briefings and technical content for the Integrated Capabilities Requirements Working Group (ICRWG)

and associated Operational Boards and participate in activities that prepare for the USCYBERCOM Requirements and Investment Board (CRIB)

2. Facilitate, coordinate, and assist in the development, review, and edit of briefings and technical content for DoD-level cyber organizations, working groups, and boards
3. Collaborate with internal USCYBERCOM and external organizations to identify capability gaps that prevent mission accomplishment
4. Synchronize and prioritize capability requirements and new tactical uses of existing capabilities across applicable staff elements, JFHQs, subordinate headquarters, Service Cyber components, CCMD, and components and agencies with cyber-related missions
5. Prepare and deliver operational capability requirements specifications and regular updates to USCYBERCOM leadership
6. Provide recommendations to developers and users on the technical aspects of cyberspace requirements
7. Identify and recommend cyberspace operations best practices, streamline processes, and methods to integrate emerging cyber technologies
8. Research capabilities to identify potential target pairing, make timely assessments on munitions effectiveness, and provide an analysis and recommendation report **(Section F.3, Deliverable 20)**
9. Recommend guidance to the field. Assist in the transition of operational capability requirements to applicable staff elements, JFHQs, subordinate headquarters, Service Cyber components, CCMD, and components and agencies with cyber-related missions
10. Support cyber capabilities and targeting gap analysis through comparison, documenting, and reporting short falls in cyber capabilities against validated targeting requirements

C.4.2.11.1 SUBTASK 2.11.1 – PERFORM CYBER REQUIREMENTS CELL (CRC) COORDINATION

The CRC coordination is a critical process regarding capabilities. The CRC coordination requires knowledge of cyber capability development processes within the IC.

The contractor shall provide the following cyber requirements CRC coordination support:

1. Participate in the NSA CRC process and collaborate with NSA for capability support requests from applicable staff elements, JFHQs, subordinate headquarters, Service Cyber components, CCMD, and components and agencies with cyber-related missions.
2. Analyze and track capability support requests sent to the CRC and maintain communication with the requesting organization until each request is fulfilled
3. Maintain and deconflict requirements of external organizations and update related databases
4. Prepare status briefs **(Section F.3, Deliverable 17)** to facilitate interagency communication on cyber capabilities

C.4.2.11.2 SUBTASK 2.11.2 – PERFORM STO/SAP CYBER CAPABILITY ANALYSIS

STO/SAP cyber capability analysis is the process of pairing operational requirements with STO/SAP capabilities. STO/SAP cyber capability analysis requires the ability to pass an

additional layer of security review and must adhere to need-to-know and material contribution criteria. The contractor will be required to become knowledgeable of capability development processes and STO/SAP capabilities IOT efficiently facilitate the process.

The contractor shall provide the following STO/SAP cyber capability analysis support:

1. Identify and develop STO/SAP cyber capability resources to address operational gaps and requirements
2. Attend and provide input to the ICRWG and associated Operational Boards IOT synchronize the collateral and STO/SAP capability development efforts
3. Brief and update STO/SAP planners on issues **(Section F.3, Deliverable 17)**; make capability improvement and development recommendations to the USCYBERCOM TPOCs
4. Maintain and update STO/SAP capability documents.

C.4.2.12 SUBTASK 2.12 – PROVIDE CYBERSPACE CAPABILITY REGISTRY (CCR) MANAGEMENT SUPPORT

The CCR is a centralized, access controlled, web-based registry containing key fact-of information on cyber capabilities developed and/or maintained throughout the DoD. CCR management provides input to operational use, requirements, and capability limitations that impact the decision and policy making processes and improves CCR usability and accessibility.

The contractor shall provide the following CCR management support:

1. Analyze user requirements for system improvements to the CCR and submit changes to the solution provider. Collaborate with the solution provider through the system lifecycle process to ensure user requirements are met
2. Review technical capability documentation upon submission to the CCR to ensure it is clear, consistent, and complete
3. Assist in establishing and implementing a maintenance program that improves the operational usefulness, fosters information operations community collaboration in the development and employment of cyber warfare capabilities
4. Assist with functional testing and recommending further development of cyber warfare capabilities that could be made operationally effective with minimal additional development
5. Review, analyze, and maintain data provided from end users and developers on their operational cyber capabilities. Recommend validation of the data for usability and/or implementation by the operational users
6. Assess performance, readiness, and reliability of the CCR and provide an analysis and recommendation report **(Section F.3, Deliverable 20)**
7. Collaborate with various internal and external cyber capability development organizations
8. Monitor the CCR; provide documented recommendations for process and procedure improvements, enhancements, and refinements, creating streamlined Quality Assurance (QA) processes that leverage the enhanced functionality of the CCR

C.4.2.13 SUBTASK 2.13 – PROVIDE CYBER JOINT MUNITIONS EFFECTIVENESS SUPPORT

The Cyber Joint Munitions Effectiveness Manual (JMEM) initiative falls under the Joint Staff program of record for non-kinetic weaponeering called the Joint Capability and Analysis Assessment System (JCAAS). J3 Fires is the Functional Area Lead (FAL) for the cyber JMEM under the Joint Targeting Coordination Group/Munitions Effectiveness (JTCG/ME). Cyber JMEM is following the kinetic model to include determining relevant weapons characteristics, targeting vulnerabilities, and developing analytical models, database, algorithms, and metrics necessary to estimate the effectiveness of specific weapons employed against specific targets in specific scenarios.

The contractor shall provide the following cyber joint munitions effectiveness support:

1. Recommend, develop, evaluate, analyze, and integrate cyber weapons/tools/capabilities
2. Act as a liaison between USCYBERCOM and the JTCG/ME PMs and their partner organizations
3. Assist in managing and running Operational User Working Groups and Functional Area Working Groups
4. Coordinate with the IC tool developers, the CMF tool developers, and other weapon/tool/capability providers
5. Coordinate with the C2 Systems, CCR managers, Cyber Network Operations Database (CNODB), Modernized Integrated Database (MIDB), and other system managers and/or engineers to link data, methodologies, and operational assessment processes
6. Assist with the project management of testing and evaluation of tools
7. Develop and propose strategic analysis of cyber weapons/tools
8. Evaluate strategic analysis of weapons/tools. Evaluate software tools to support the strategic analysis of data and the dissemination of analysis data
9. Assist in identifying gaps in cyber weapons/tools/capabilities. Develop and propose Mission Needs Statements (MNS) based on the identified gaps
10. Evaluate and integrate existing network analysis tools and software and related system media analysis tools and software databases
11. Develop SOPs and assist in the development of CONOPs that describe weapon/capability/tool functionality and operational capabilities **(Section F.3, Deliverable 21)**

C.4.3 TASK 3 – PROVIDE CYBERSPACE PLANNING SUPPORT

The JOPP spans both the J3 and J5 directorates of USCYBERCOM. The USCYBERCOM J3 plans, coordinates, integrates, synchronizes, and conducts activities directing the operation and defense of the DODIN and, when directed, plans the conduct of full spectrum military Cyberspace Operations IOT enable actions in all domains, ensure U.S./Allied freedom of action in cyberspace, and deny the same to our adversaries.

Cyber research, analysis, and recommendations for the integration of cyber include: Operations Plan (OPLAN) development, intelligence and analysis requirements definition, cyber assessment

development, information operations integration, STO, SAP cyber capabilities coordination, and Evaluation Request and Response Messages (EReqM and EResM, respectively) integration.

The contractor shall provide the following cyberspace planning support:

1. Provide cyber analysis and develop documentation necessary for USCYBERCOM to develop future CCMD's campaign plans, operational, and contingency plans
2. Collect, analyze, and disseminate future processes and procedures to ensure the confidentiality, integrity, and availability of data related to network operations and warfare
3. Coordinate, deconflict, and facilitate communications with all applicable staff elements, JFHQs, subordinate headquarters, Service Cyber components, CCMD, components, and agencies with cyber-related missions
4. Ensure network operation plans are synchronized with major military exercises
5. Participate in cyber COA development for Cyberspace Operations to deter attacks against the DODIN
6. Assist in identifying and developing requirements, making recommendations for the prioritization of requirements for development
7. Assist in developing network operation plans, including identification and development of USCYBERCOM mission enhancement opportunities
8. Report on evolving cyber policies and cyber security trends that effect USCYBERCOM's ability to defends its networks
9. Review and evaluate cyber policy directives/documents and issue papers
10. Provide the information security and assurance analysis necessary to development of cyber TTPs, CONOPs, and SOPs
11. Review and assess existing DoD cyber documentation, cyber wargame reports, TTPs, and lessons learned, and provide an analysis and recommendation report **(Section F.3, Deliverable 20)**
12. Provide the technical research, analysis, and recommendations for USCYBERCOM to develop cyberspace COAs, CONOPs, and TTPs IOT support Cyberspace Operations
13. Provide an analysis and recommendation report **(Section F.3, Deliverable 20)** on the synchronization of Cyberspace Operations with the collection, review, and assessment of existing DoD and service cyber documentation, exercise, and event scenario reports, CONOPs, TTPs, and lessons learned
14. Design and develop cyber technical and analytical documents for designated USCYBERCOM Cyberspace Operations efforts involving the following:
    a. Cyber collaboration among DoD and other organizations with cyber-related missions
    b. Standard approval processes for Cyberspace Operations
    c. Cyber deconfliction, coordination, and assessment policies and processes, and full spectrum cyberspace coordination and reporting procedures.

C.4.4 TASK 4 – PROVIDE CYBERSPACE TRAINING AND EXERCISES SUPPORT

The contractor shall provide support to USCYBERCOM training and exercises, and JOSG-sponsored exercises. The JOSG is responsible for conducting tabletop exercises (TTXs) to

validate each stage of JIE implementation. As part of the exercise approach, the JOSG produces deliverables for the PCC, including assessment plans, test reports, and after action reports.

The contractor shall provide the following cyberspace training and exercises support:

1. Plan, organize, coordinate and participate in JOSG TTXs and other similar JIE events. The Government anticipates contractor support to approximately 6-10 exercises/events on an annual basis
2. Coordinate with JIE partners and stakeholders to develop and plan scenarios to meet JIE exercise objectives
3. Develop documents to include after action reports **(Section F.3, Deliverable 18)**, results and conclusions with relevant organizations such as DoD organizations, Federal Agencies, and commercial partners
4. Conduct post-exercise lessons learned studies and develop COAs in response to JOSG training objectives
5. Coordinate with the USCYBERCOM J7 Directorate to ensure JIE exercise activities adhere to USCYBERCOM exercise plans, policies, and procedures
6. Conduct technical research, analysis, and provide recommendations **(Section F.3, Deliverable 20)** for the JOSG to support Joint Event Lifecycle (JELC) Events including CCMD exercises, TTXs, and scenario development/synchronization
7. Identify, track, and resolve issues impacting training, exercises, and daily operations
8. Collaborate with J7 elements to establish overall objectives, priorities, and plans for the USCYBERCOM's joint exercise program, assuring focus on issues and challenges critical to pursuit of Cyberspace Operations
9. Coordinate with partners and stakeholders in the application of analytical methodologies to assess MOEs and MOPs for operational scenarios

C.4.5 TASK 5 – STRATEGY/POLICY/DOCTRINE DEVELOPMENT AND CAMPAIGN ASSESSMENTS

The contractor shall contribute to the development of policies and governing directives to secure, operate, and defend the DODIN and to conduct cyberspace operations. The contractor shall coordinate with Joint Staff, OSD, DoD CIO, DoD Components and the IC to assist with establishing, reviewing, and adjudicating cyberspace policies and directives.

C.4.5.1 SUBTASK 5.1 – JIE STRATEGIC SUPPORT

JIE Strategic support encompasses strategic-level planning and the synchronization of activities across all JOSG lines of operations, and in coordination with the components, to implement the Secretary of Defense's (SecDef's) objectives.

The contractor shall provide the following JIE Strategic support:

1. Plan, organize, determine, and recommend necessary policies, regulations, directives, programs, doctrine, and procedures for the establishment and maintenance of assigned and anticipated changes to the DODIN ISO JIE **(Section F.3, Deliverable 21)**
2. Draft plans assist in the development of CONOPS required to execute the JIE

3. Assist the oCIO JIE governance team in formulating policy; assist with writing, analyzing, and consolidating feedback on all JIE-specific policies
4. Analyze DoD and government policies and provide an analysis and recommendation report **(Section F.3, Deliverable 20)** to those policies to support the JIE implementation process
5. Develop white papers **(Section F.3, Deliverable 19)**, compliance reports, and assessment reports ISO activities for defining strategy, policy, and doctrine for JIE
6. Assist in the development and refinement of the JIE C2 Construct and the JIE Operational CONOPs
7. Organize, coordinate, and participate in JIE working groups and other JIE workshop-type of events
8. Develop and conduct update briefs, presentations, and papers to USCYBERCOM leadership to ensure situational awareness and status are conveyed related to the assigned project areas **(Section F.3, Deliverable 17)**

C.4.6 TASK 6 – PROVIDE INFORMATION TECHNOLOGY (IT)/ COMMUNICATIONS (COMMS) SUPPORT

USCYBERCOM J3 is responsible for identifying requirements and concepts of operation which enable and align with the C2 and defense of the DODIN. Supporting this task requires duties such as system evaluations, system analysis, and infrastructure assessments. Additionally, this task requires knowledge of planning and engineering of enterprise architectures management of system configuration, system administration support, and system engineering support.

The contractor shall provide the following IT/Comms support:

1. Contribute to the design and development of systems and associated enterprise architectures
2. Review and provide comments on technical materials consisting of, but not limited to, technical documentation and reports, cyber policy and procedures, and planning materials
3. Provide technical edits to engineering documentation, software documentation, manuals, reports, or any other documents or presentations
4. Coordinate and collaborate with the USCYBERCOM C4IT Directorate (J6) to ensure seamless integration and management of services, systems, and networks into existing and future joint DODIN infrastructure
5. Analyze and assess enterprise architecture design and development proposals and provide an analysis and recommendations report **(Section F.3, Deliverable 20)**
6. Assist in collecting and organizing information required for preparation of documents, training materials, guides, proposals, and reports
7. Develop program, system, operations, implementation, and user documentation
8. Develop concept papers, technical white papers **(Section F.3, Deliverable 19)**, and related documentation detailing network practices for implementation throughout the DoD
9. Provide detailed hands-on training and training documentation to include system capabilities and functionality, system logon/logoff procedures, understanding of data

fields, information processing, report production, file retrieval, system security features, and system error messages

C.4.6.1 SUBTASK 6.1 – PROVIDE FIRES AND EFFECTS C2 SYSTEM DEVELOPMENT SUPPORT

The Fires & Effects C2 System Development task requires an extensive knowledge, understanding and familiarity of the Joint Targeting Cycle and the JOPP. This task requires knowledge, understanding, and the ability to explain C2 of Cyberspace Operations to include the CTO development and execution, Cyber Effects Request Forms (CERFs), Joint Tactical Cyber Requests, and the Cyber Tasking Cycle. Additionally, this task requires the understanding and the ability to develop applications and systems IAW Section 508 compliance.

The contractor shall provide the following fires and effects C2 system development support:

1. Provide C2 systems development, management, and systems engineering support to network and Web-based initiative functions of the Government, executed in real time
2. Develop and maintain Government C2 Systems across multiple platforms to suit real-time operational needs
3. Provide database administration related information security and maintenance, as needed, ISO evolving C2 systems
4. Provide real-time Cyber C2 system support and system administration for exercises, crisis, or contingencies (this could be a 24x7 on-call-type position)
5. Review functional requirements with other technical experts for feasibility in implementing technical solutions for USCYBERCOM, including requirements analysis, and provide recommendations to the Government on implementing solutions

C.4.6.2 SUBTASK 6.2 – PROVIDE COMMAND HIGH INTEREST PROJECT SUPPORT (OPTIONAL)

The USCYBERCOM Command High Interest Projects Group plans, develops, and implements the Commander's highest priorities and future concepts. The Command High Interest Projects Group integrates, informs, and influences cross-directorate activities, provides command integration and synchronization for high interest projects. These projects may include: strategic planning, research and evaluation, strategic analysis and synthesis, key engagement and initiatives, and communication and command strategic messaging.

The contractor shall provide the following Command high interest project support:

a. Contribute to the design and development of systems and associated enterprise architectures
b. Develop technical papers, white papers **(Section F.3, Deliverable 19)**, and reports **(Section F.3, Deliverable 17)**, and assist in the development of CONOPS
c. Identify and develop requirements
d. Develop system and operational views, diagrams, system architecture, network diagrams, and network architectures
e. Review and provide comments on technical materials consisting of, but not limited to, technical documentation and reports, cyber policy and procedures, and planning materials

f. Develop engineering documentation, system documentation, manuals, reports, or any other documents or presentations
g. Assist in collecting and organizing information required for preparation of briefs, documents, training materials, guides, and reports **(Section F.3, Deliverable 17)**
h. Develop program, system, operations, implementation, governance, and user documentation
i. Coordinate and communications with all applicable staff elements, JFHQs, subordinate headquarters, Service Cyber components, CCMD, components, and agencies with cyber-related missions.

C.4.7 TASK 7 – PROVIDE BUSINESS AREA SUPPORT

C.4.7.1 SUBTASK 7.1 – PROVIDE ADMINISTRATIVE SUPPORT

Administrative support is critical to the effective and efficient operations of the USCYBERCOM. Administrative support includes all aspects of administrative management, general office support, and coordination among organizations for day-to-day operations.

The contractor shall provide the following business administration support:

1. Plan and organize daily activities in coordination with internal and external entities for day-to-day operations
2. Schedule and coordinate meetings, visits, and events, and prepare supporting briefs and reports **(Section F.3, Deliverable 17)**
3. Prepare, process, and track correspondence
4. Prepare and distribute meeting agendas and meeting minutes /notes and track action items
5. Track ancillary training requirements
6. Reserve meeting space and facilitate audio visual and telecommunication support for scheduled meetings
7. Produce and distribute the battle rhythms, activity reports, and staff meeting briefs
8. Maintain and update schedules, calendars, and the personnel accountability tracker for daily work status
9. Assist in preparing the office for office relocation and/or building move
10. Monitor, update, and report on the status of assigned Workflow Management System (WMS) tasks assigned **(Section F.3, Deliverable 17)**. WMS is a web-based system that enables organizations within USCYBERCOM to task, track, and manage tasks.

C.4.7.2 SUBTASK 7.2 – PROVIDE KNOWLEDGE MANAGEMENT SUPPORT

Knowledge Management is essential to conduct operations in USCYBERCOM. Knowledge Management enables collaboration of cyber operational data, and provides USCYBERCOM leadership with relevant information to make informed decisions. The contractor shall coordinate activities with the USCYBERCOM Chief Knowledge Officer (CKO) to ensure continued compliance with Command policies and procedures. The contractor shall utilize information sharing portals to have information readily accessible to USCYBERCOM and external stakeholders. The contractor shall provide expertise in developing MS SharePoint portals, database management, and MS office suite applications.

The contractor shall provide the following knowledge management support:

1. Post, edit, distribute, and maintain appropriate content on USCYBERCOM classified and unclassified website/portals
2. Develop and maintain an accurate, consistent, repeatable process for responses to official questions through Request for Information (RFI) tools by collecting, consolidating, and preparing written responses to external RFI or internal query from USCYBERCOM leadership
3. Create and maintain records in compliance with DoD Records Management policies and directives
4. Organize data, establish file structures, and ensure information is captured and stored in locations accessible to various user groups
5. Develop TTPs for coordinating the flow of information and work with USCYBERCOM training branches to periodically test these TTPs during exercises

C.4.7.3 SUBTASK 7.3 – PROVIDE REQUIREMENTS MANAGEMENT SUPPORT FOR FIRES AND EFFECTS C2 SYSTEM DEVELOPMENT

The Fires & Effects C2 System Development requires requirements management support for Cyber Command and Control Portal for Operations (C3PO) and future C2 systems adopted by the command. C3PO is the current system mandated for use by the CMF to implement the Cyber Tasking Cycle. The contractor shall provide advice and guidance on other C2 systems capabilities and usage.

The contractor shall provide the following project support for fires and effects C2 system development:

1. Assist with end-to-end technical requirement lifecycle of C3PO and future C2 systems
2. Identify, analyze, and refine initial requirements for C3PO and future C2 systems
3. Recommend priorities for USCYBERCOM's operational requirements regarding C3PO and future C2 systems
4. Analyze requirements and develop various levels of system requirements and documentation development required for the design and build of a solution for C2 problem sets
5. Assist in integrating selected C3PO and future C2 systems with selected situational awareness systems to include providing documentation.

C.4.7.4 SUBTASK 7.4 - PROVIDE JIE PROJECT MANAGEMENT SUPPORT

The contractor shall provide the following JIE project management support:

1. Assist the Government in preparing or conducting briefings on program related activities
2. Develop and maintain work breakdown structures and integrated master schedules
3. Perform evaluations of existing procedures, processes, techniques, models, and/or systems to identify areas for improvement and recommend solutions
4. Interface with partners and stakeholders to perform enterprise-wide horizontal integration planning
5. Perform program management to control risk, mitigate schedule delay
6. Assist with the review of risk and risk mitigation activities

7. Recommend prioritization of tasks
8. Analyzing validated and prioritized requirements to manage timelines and risks
9. Maintaining JIE project information and status of ongoing project activities
10. Analyzing and refining initial user needs and assist in defining requirements
11. Collaborating with teams managing related and dependent tasks to maintain status of collective progress
12. Developing courses of action to fulfill gaps and requirements.

C.4.7.5 SUBTASK 7.5 – PROVIDE BUSINESS PROCESS RE-ENGINEERING (BPR) SUPPORT (OPTIONAL)

BPR is the analysis and redesign of workflows within and between organizations. The J3 uses BPR to implement changes in processes such as operational priorities, requirements management, mission management, operational assessments, and event/incident response. BPR requires the knowledge of several BPR theories and change management methods IOT make the most efficient recommendations to the USCYBERCOM.

The contractor shall provide the following BPR support:

1. Interview personnel within various Directorates, subordinate units, and appropriate external units to determine processes, including expected inputs and outputs versus actual inputs and outputs
2. Analyze processes in the command and subordinate units develop an analysis and recommendation report **(Section F.3, Deliverable 20)** that identifies weaknesses, areas to sustain, and areas of improvement based upon proven methods
3. Make recommendations to the USCYBERCOM leadership on process changes to optimize efficiency and increase accurate productivity.

C.4.7.6 SUBTASK 7.6 – PROVIDE GRAPHIC ARTS SUPPORT (OPTIONAL)

The contractor shall design graphical presentations utilizing products including MS Office (especially PowerPoint) and Adobe Creative Suite ISO the USCYBERCOM J3 **(Section F.3, Deliverable 17)**. The contractor shall create concepts from start to finish in a collaborative environment with attention to detail. The contractor shall display creativity in designs, layout, and display.

C.4.8 TASK 8 – PROVIDE CYBER OPERATIONS SURGE SUPPORT (OPTIONAL)

The Government anticipates surge support will be required on a case-by-case basis when there are specific Cyberspace Operations events that require increased support. The Government reserves the right to exercise surge support services at any point in time during a TO performance, IAW the terms and conditions of the contract. In the occurrence of a crisis action matter, USCYBERCOM may require surge support to respond to a crisis and unknown cyber threats. The duration of surge support during the TO PoP may or may not be determined by USCYBERCOM at the time of occurrence. The surge support shall be required for the duration of the crisis action matter, as defined by appropriate authoritative documents. The surge support shall not result in a decrease of support to other TO requirements unless approved by the CO and COR. The Government anticipates that annually surge events will represent approximately five percent of the level of effort required for Tasks 1 through 7.

The following applies to performing the surge support requirements:

1. The Government will determine the amount of surge support required at the time of the crisis action matter. Each crisis action matter may require a different amount of surge support
2. The contractor shall respond to providing surge support in response to identified crisis action matters with the urgency the matter entails. Surge support may be required to be staffed and worked within USCYBERCOM spaces, following the first notification informing the contractor of a request for surge support
3. Once a crisis action matter has been declared ended, the contractor shall proceed with an orderly and efficient transition-out period not to exceed thirty days. During the transition-out period, the contractor shall fully cooperate with, and assist the Government with, activities closing out the crisis action matter, developing required documentation, transferring knowledge, and lessons learned

SECTION D - PACKAGING AND MARKING

NOTE: Section D of the Contractor's MA IDIQ is applicable to this TO and is hereby incorporated by reference.

This page intentionally left blank.

SECTION E - INSPECTION AND ACCEPTANCE

NOTE: Section E of the Contractor's MA IDIQ is applicable to this TO and is hereby incorporated by reference. In addition, the following applies:

E.1 PLACE OF INSPECTION AND ACCEPTANCE

Inspection and acceptance of all work performance, reports, and other deliverables under this TO shall be performed by the FEDSIM COR and the USCYBERCOM TPOC.

E.2 SCOPE OF INSPECTION

All unclassified deliverables will be inspected for content, proper classification markings, completeness, accuracy, and conformance to TO requirements by the FEDSIM COR and TPOC. All classified deliverables will be inspected for content, proper classification, markings, completeness, accuracy and conformance to TO requirements by the TPOC. Inspection may include validation of information or software through the use of automated tools, testing, or inspections of the deliverables, as specified in the TO. The scope and nature of this inspection will be sufficiently comprehensive to ensure the completeness, quality, and adequacy of all deliverables.

The Government requires a period NTE 15 workdays after receipt of final deliverable items for inspection and acceptance or rejection.

E.3 BASIS OF ACCEPTANCE

The basis for acceptance shall be compliance with the requirements set forth in the TO, the contractor's proposal, and relevant terms and conditions of the contract. Deliverable items rejected shall be corrected in accordance with the applicable clauses.

Reports, documents, and narrative-type deliverables will be accepted when all discrepancies, errors, or other deficiencies identified in writing by the Government have been corrected.

If the draft deliverable is adequate, the Government may accept the draft and provide comments for incorporation into the final version.

All of the Government's comments on deliverables must either be incorporated in the succeeding version of the deliverable, or the contractor must explain to the Government's satisfaction why such comments should not be incorporated.

If the Government finds that a draft or final deliverable contains spelling errors, grammatical errors, or improper format, or otherwise does not conform to the requirements stated within this TO, the document may be immediately rejected without further review and returned to the contractor for correction and resubmission. If the contractor requires additional Government guidance to produce an acceptable draft, the contractor shall arrange a meeting with the TPOC and the FEDSIM COR.

E.4 DRAFT DELIVERABLES

The Government will provide written acceptance, comments, and/or change requests, if any, within 15 workdays (unless specified otherwise in **Section F**) from Government receipt of the draft deliverable. Upon receipt of the Government's comments, the contractor shall have ten workdays to incorporate the Government's comments and/or change requests and to resubmit the deliverable in its final form.

E.5 WRITTEN ACCEPTANCE/REJECTION BY THE GOVERNMENT

The Government will provide written notification of acceptance or rejection **(Section J, Attachment D)** of all final deliverables within 15 workdays (unless specified otherwise in Section F). All notifications of rejection will be accompanied with an explanation of the specific deficiencies causing the rejection.

E.7 NON-CONFORMING PRODUCTS OR SERVICES

Non-conforming products or services will be rejected. Deficiencies will be corrected, by the contractor, within ten workdays of the rejection notice. If the deficiencies cannot be corrected within 10 workdays, the contractor shall immediately notify the FEDSIM COR of the reason for the delay and provide a proposed corrective action plan within ten workdays.

If the contractor does not provide products or services that conform to the requirements of this TO, the Government will not pay the cost associated with the non-conforming products or services.

SECTION F – DELIVERABLES OR PERFORMANCE

NOTE: Section F of the Contractor's MA IDIQ is applicable to this TO and is hereby incorporated by reference. In addition, the following applies:

F.1 PERIOD OF PERFORMANCE

The PoP for this TO is a one-year base period and four, one-year option periods.

F.2 PLACE OF PERFORMANCE

The primary place of performance is Fort George G. Meade, Maryland. As a contingency and ISO the Continuity of Operations Plan (COOP), the contractor may be required to work from an alternate place of performance or the contractor site. Long-distance Continental United States (CONUS) and Outside the Continental United States (OCONUS) travel is anticipated ISO this effort. Program Management support may be provided at the contractor's location. Under NO CIRCUMSTANCE will a home office be considered an alternate work location.

F.3 DELIVERABLES

The following schedule of milestones will be used by the FEDSIM COR to monitor timely progress under this TO. For proposal purposes, offerors shall use June 30, 2016, as the project start date.

The following abbreviations are used in this schedule:

NLT: No Later Than

TOA: Task Order Award

All references to Days: Government Workdays

Deliverables are due the next Government workday if the due date falls on a holiday or weekend.

The contractor shall submit the deliverables listed in the following table:

DEL. #	MILESTONE/ DELIVERABLE	TOR REFERENCE	PLANNED COMPLETION DATE	DATA RIGHTS CLAUSE FAR 52.227-14
0	Project Start		10 days after Award	
1	Project Kick-Off Meeting	C.4.1.1	Within 10 days of Project Start	
2	Kick-Off Agenda	C.4.1.1	Within 10 days of Project Start	X
3	Kick-Off Meeting Presentation	C.4.1.1	Within 10 days of Project Start	X
4	Kick-Off Meeting Report	C.4.1.1	5 days following Kick-Off Meeting	X

DEL. #	MILESTONE/ DELIVERABLE	TOR REFERENCE	PLANNED COMPLETION DATE	DATA RIGHTS CLAUSE FAR 52.227-14
5	Monthly Status Report	C.4.1.2	Monthly, on the 10th of each month	X
6	PMP - Draft	C.4.1.4	Within 20 days of Project Start	X
7	PMP - Final	C.4.1.4	Within 5 days of receiving Government comments	X
8	PMP - Update	C.4.1.5	Annually, at minimum	X
9	Trip Report(s)	C.4.1.6	Within 5 days of trip completion	X
10	Meeting Reports	C.4.1.7	5 days following the subject meeting	X
11	QCP - Draft	C.4.1.8	At time of proposal submission	X
12	QCP - Final	C.4.1.8	Within 15 days of Project Start	X
13	QCP - Update	C.4.1.8	Annually, at minimum	X
14	Transition-In Plan - Draft	C.4.1.9	At time of proposal submission	X
15	Transition-In Plan - Final	C.4.1.9	Within 5 days of Project Start	X
16	Transition-Out Plan	C.4.1.10	90 calendar days prior to the expiration of the TO	X

DEL. #	MILESTONE/ DELIVERABLE	TOR REFERENCE	PLANNED COMPLETION DATE	DATA RIGHTS CLAUSE FAR 52.227-14
17	Status and Situational Awareness Briefs/Presentations	C.4.2.4, C.4.2.5.2, C.4.2.6, C.4.2.6.1, C.4.2.7, C.4.2.8, C.4.2.9, C.4.2.11, C.4.2.11.1, C.4.2.11.2, C.4.5.1, C.4.6.2, C.4.7.1, and C.4.7.6	In accordance with PMP	X
18	After Action Reports	C.4.2.1.2, C.4.2.5.2, and C.4.4	In accordance with PMP	X
19	White Papers	C.4.2.1, C.4.2.1.1, C.4.2.1.2, C.4.2.1.3, C.4.2.7, C.4.5.1, C.4.6, and C.4.6.2	In accordance with PMP	X

DEL. #	MILESTONE/ DELIVERABLE	TOR REFERENCE	PLANNED COMPLETION DATE	DATA RIGHTS CLAUSE FAR 52.227-14
20	Analysis and Recommendation Reports	C.4.2(2), C.4.2(5), C.4.2.1.3 C.4.2.1, C.4.2.1.3, C.4.2.4, C.4.2.4.2, C.4.2.5, C.4.2.5.3, C.4.2.7, C.4.2.8, C.4.2.9, C.4.2.11, C.4.2.12, C.4.3, C.4.4, C.4.5.1, and C.4.6	In accordance with PMP	X
21	Processes and Procedures, Standard Operating Procedures (SOPs)	C.4.2.4.1, C.4.2.4.2, C.4.2.7, C.4.2.8, C.4.2.10, C.4.2.13, C.4.5.1	In accordance with PMP	X
22	Redacted TO	F.4	Within 10 days of TO or modification award	X

The contractor shall mark all deliverables listed in the above table to indicate authorship by contractor (i.e., non-Government) personnel; provided, however, that no deliverable shall contain any proprietary markings inconsistent with the Government's data rights set forth in this TO. The Government reserves the right to treat non-confirming markings in accordance with subparagraphs (e) and (f) of the FAR clause at 52.227-14. The contractor shall also mark each deliverable with proper security markings IAW Controlled Access Program Coordination Office's (CAPCO) Authorized Classification and Control Markings.

F.3.1 DELIVERABLE FORMATS

DEL. #	DELIVERABLE	MINIMUM CONTENT	MINIMUM LENGTH	SUBMISSION METHOD	FORMAT

DEL. #	DELIVERABLE	MINIMUM CONTENT	MINIMUM LENGTH	SUBMISSION METHOD	FORMAT
10	Meeting Reports	i. Summary ii. Potential Problem Areas iii. Direction of Meeting A. Areas for Future Participation iv. Recommendations for actionable items	a. 1 page, no more than 2 pgs	Electronic	Fully Edited Contractor Final Iteration
18	After Action Reports	i. Purpose ii. Attendee(s) iii. Agenda iv. Discussion Areas v. Issues vi. Pending/ Completed Actionable Items vii. Conclusion	1 page, single spaced, 12 Font, 8.5 x 11 paper	Electronic	Fully Edited Contractor Final Iteration
19	White Papers	i. Technical communication capable of representing a Division or Organization's position, opinion or status on complex topics ii. Technically and topically accurate iii. Targets, intended audience	a. 1 page, single spaced, 12 font, 8.5 x 11 paper	Electronic	Fully Edited Contractor Final Iteration

DEL. #	DELIVERABLE	MINIMUM CONTENT	MINIMUM LENGTH	SUBMISSION METHOD	FORMAT
20	Analysis and Recommendation Reports	i. Technical communication capable of representing a Division or Organization's position, opinion or status on complex topics ii. Technically and topically accurate iii. Targets, intended audience	a. 1 page, single spaced, 12 font, 8.5 x 11 paper	Electronic	Fully Edited Contractor Final Iteration

F.4 PUBLIC RELEASE OF CONTRACT DOCUMENTS REQUIREMENT

The contractor agrees to submit, within 10 workdays from the date of the CO's execution of the TO, or any modification to the TO (exclusive of Saturdays, Sundays, and Federal holidays), a portable document format (PDF) file of the fully executed document with all proposed necessary redactions, including redactions of any trade secrets or any commercial or financial information that it believes to be privileged or confidential business information, for the purpose of public disclosure at the sole discretion of GSA **(Section F.3, Deliverable 22)**. The contractor agrees to provide a detailed written statement specifying the basis for each of its proposed redactions, including the applicable exemption under the Freedom of Information Act (FOIA), 5 U.S.C. § 552, and, in the case of FOIA Exemption 4, 5 U.S.C. § 552(b)(4), shall explain why the information is considered to be a trade secret or commercial or financial information that is privileged or confidential. Information provided by the contractor in response to the contract requirement may itself be subject to disclosure under the FOIA. Submission of the proposed redactions constitutes concurrence of release under FOIA.

GSA will carefully consider all of the contractor's proposed redactions and associated grounds for nondisclosure prior to making a final determination as to what information in such executed documents may be properly withheld.

F.5 DELIVERABLES MEDIA

The contractor shall deliver all electronic versions by email, as well as placing in USCYBERCOM's designated repository. The following are the required electronic formats, whose versions must be compatible with Microsoft Office versions utilized by USCYBERCOM.

a. Text MS Word

b. Spreadsheets MS Excel

c.	Briefings	MS PowerPoint
d.	Drawings	MS PowerPoint (preferred), MS Visio
e.	Schedules	MS Excel (preferred), MS Project

F.6 PLACE(S) OF DELIVERY

Unclassified deliverables and correspondence shall be delivered to the FEDSIM COR and USCYBERCOM TPOC specified in individual task orders. Classified deliverables shall be delivered to the USCYBERCOM TPOC and notice of the delivery shall be provided to the CO and FEDSIM COR.

Unclassified deliverables or correspondence shall be delivered to the FEDSIM COR at the following address:

GSA FAS AAS Federal System and Integration Management Center (FEDSIM)
ATTN: Donna Young, FEDSIM COR
1800 F Street, NW
Suite 3100 (QF0B)
Washington, D.C. 20405
Telephone: (478) 893-0619
Email: donna.young@gsa.gov

Copies of all deliverables shall also be delivered to the USCYBERCOM TPOC at the following address:

Provided after award

F.7 NOTICE REGARDING LATE DELIVERY/PROBLEM NOTIFICATION REPORT (PNR)

The contractor shall notify the FEDSIM COR via a Problem Notification Report (PNR) (**Section J, Attachment E**) as soon as it becomes apparent to the contractor that a scheduled delivery will be late. The contractor shall include in the PNR the rationale for late delivery, the expected date for the delivery, and the project impact of the late delivery. The FEDSIM COR will review the new schedule and provide guidance to the contractor. Such notification in no way limits any Government contractual rights or remedies including, but not limited to, termination.

NOTE: Section G of the Contractor's MA IDIQ is applicable to this TO and is hereby incorporated by reference. In addition, the following applies:

G.1 CONTRACTING OFFICER'S REPRESENTATIVE (COR)

The CO appointed a COR in writing through a COR Appointment Letter (**Section J, Attachment B**). The FEDSIM COR will receive, for the Government, all work called for by the TO and will represent the CO in the technical phases of the work. The FEDSIM COR will provide no supervisory or instructional assistance to contractor personnel.

The FEDSIM COR is not authorized to change any of the terms and conditions, scope, schedule, and price of the TO. Changes in the scope of work will be made only by the CO by properly executed modifications to the TO.

G.1.1 CONTRACT ADMINISTRATION

Contracting Officer:

Robert Wade
GSA FAS AAS FEDSIM
1800 F Street, NW
Suite 3100 (QF0B)
Washington, D.C. 20405
Telephone: (202)-603-0283
Email: Robert.wade@gsa.gov

Contracting Officer's Representative:

Donna Young
GSA FAS AAS FEDSIM
1800 F Street, NW
Suite 3100 (QF0B)
Washington, D.C. 20405
Telephone: (478) 893-0619
Email: donna.young@gsa.gov

Technical Point of Contact:

Provided after award.

G.2 INVOICE SUBMISSION

The contractor shall submit Requests for Payments in accordance with the format contained in General Services Administration Acquisition Manual (GSAM) 552.232-25, PROMPT PAYMENT (NOV 2009), to be considered proper for payment. In addition, the following data elements shall be included on each invoice:

Task Order Number: (from GSA Form 300, Block 2)
Paying Number: (ACT/DAC NO.) (From GSA Form 300, Block 4)
FEDSIM Project Number: (Fill in project number)
Project Title: (Fill in project title)

The contractor shall certify with a signed and dated statement that the invoice is correct and proper for payment.

The contractor shall submit invoices as follows:

The contractor shall utilize FEDSIM's electronic Assisted Services Shared Information System (ASSIST) to submit invoices. The contractor shall submit invoices electronically by logging onto the following link (requires Internet Explorer to access the link):

https://portal.fas.gsa.gov

Log in using your assigned ID and password, navigate to the order against which you want to invoice, click the Invoices and Acceptance Reports link in the left navigator, and then click the *Create New Invoice* button. The AASBS Help Desk should be contacted for support at 877-472-4877 (toll free) or by email at AASBS.helpdesk@gsa.gov. By utilizing this method, no paper copy of the invoice shall be submitted to GSA FEDSIM or the GSA Finance Center. However, the FEDSIM COR may require the contractor to submit a written "hardcopy" invoice with the client's certification prior to invoice payment.

G.3 INVOICE REQUIREMENTS

The contractor shall submit simultaneous copies of the invoice to both the FEDSIM COR and USCYBERCOM TPOC, along with all backup documentations (e.g., receipts, credit card transactions reports, proof of indirect rates, and monthly expenditure report) prior to its submission in ASSIST. The contractor shall:

a. Combine CPFF and NTE charges (travel, tools and ODCs) in one invoice submission
b. Provide receipts for all travel and tools and ODC purchases

The contractor may invoice the fixed fee on a monthly basis. The monthly fixed fee invoiced shall be proportionate to the amount of labor expended for the month invoiced. The contractor shall address each contract type separately in the invoice submission.

The final invoice is desired to be submitted within six months of project completion. The contractor shall provide the Government with a monthly status on when the final invoice will be submitted to the Government.

G.3.1 COST-PLUS-FIXED-FEE (CPFF) CLINs (FOR LABOR)

The contractor may invoice monthly on the basis of cost incurred for the CPAF CLINs. The invoice shall include the period of performance covered by the invoice and the CLIN number and title. All hours and costs shall be reported by CLIN element (as shown in Section B), by contractor employee, and shall be provided for the current billing month and in total from project inception to date. The contractor shall provide the invoice data in spreadsheet form with the following detailed information. The listing shall include separate columns and totals for the current invoice period and the project to date.

a. Employee name (current and past employees)
b. Employee company labor category
c. Employee Alliant labor category
d. Monthly and total cumulative hours worked by task and CLIN

e. Corresponding TO Proposed rate
f. Cost incurred not billed by task and CLIN
g. Current approved forward pricing rate agreement in support of indirect costs billed

All cost presentations provided by the contractor shall also include Overhead charges and General and Administrative charges at a minimum at the cost center level and shall also include the Overhead and General and Administrative rates being applied.

The contractor may invoice after accepting the modification which includes the award fee determination and any corresponding deobligation of unearned fee. See the Award Fee Determination Plan in Section J, Attachment H for additional information on the award fee determination process.

G.2.1.2 TOOLS AND OTHER DIRECT COSTS (ODCS)

The contractor may invoice monthly on the basis of cost incurred for the Tool and ODC CLINs. The invoice shall include the period of performance covered by the invoice and the CLIN number and title. In addition, the contractor shall provide the following detailed information for each invoice submitted, as applicable. Spreadsheet submissions are required.

a. Tools and/or ODCs purchased
b. Consent to Purchase number or identifier
c. Date accepted by the Government
d. Associated CLIN
e. Project-to-date totals by CLIN
f. Cost incurred not billed
g. Remaining balance of the CLIN

All cost presentations provided by the contractor shall also include Overhead charges, General and Administrative charges and Fee in accordance with the contractor's Defense Contract Audit Agency (DCAA) cost disclosure statement.

G.2.1.3 TRAVEL

Long distance travel is defined as travel over 50 miles from the primary place of performance. Local travel will not be reimbursed.

Contractor costs for travel will be reimbursed at the limits set in the following regulations (see FAR 31.205-46):

a. Joint Travel Regulation (JTR) - prescribed by the GSA, for travel in the contiguous U.S.
b. Federal Travel Regulation (FTR) Volume 2, DoD Civilian Personnel, Appendix A - prescribed by the DoD, for travel in Alaska, Hawaii, and outlying areas of the U.S.
c. Department of State Standardized Regulations (DSSR) (Government Civilians, Foreign Areas), Section 925, "Maximum Travel Per Diem Allowances for Foreign Areas" - prescribed by the Department of State, for travel in areas not covered in the FTR or JTR.

The contractor may invoice monthly on the basis of cost incurred for cost of travel comparable with the JTR/ FTR/DSSR. The invoice shall include the period of performance covered by the

invoice, the CLIN number and title. Separate worksheets, in MS Excel format, shall be submitted for travel.

CLIN/Task Total Travel: This invoice information shall identify all cumulative travel costs billed by CLIN/Task. The current invoice period's travel details shall include separate columns and totals and include the following:

a. Travel Authorization Request number or identifier, approver name, and approval date
b. Current invoice period
c. Names of persons traveling
d. Number of travel days
e. Dates of travel
f. Number of days per diem charged
g. Per diem rate used
h. Total per diem charged
i. Transportation costs
j. Total charges
k. Explanation of variances exceeding 10 percent of the approved versus actual costs
l. Indirect handling rate

All cost presentations provided by the contractor shall also include Overhead charges and General and Administrative charges in accordance with the contractor's DCAA cost disclosure statement.

NOTE: Section H of the Contractor's MA IDIQ is applicable to this TO and is hereby incorporated by reference. Section numbers align with the MA IDIQ. In addition, the following applies:

H.1 KEY PERSONNEL

The following are the minimum personnel who shall be designated as "Key." The Government does not intend to dictate the composition of the ideal team to perform this TO.

1. Project Manager (PM)
2. Cyberspace Joint Operations Planner Lead
3. Weapons & Capabilities Lead
4. JOSG Lead
5. Cyberspace Operations Lead

The Government desires that Key Personnel be assigned for the duration of the TO.

All Key Personnel are required to possess the following qualifications:

1. Strong attention to detail and organizational skills
2. Excellent communications skills
3. Strong analytical and problem solving skills
4. Proficient in MS Office applications (e.g., Word, PowerPoint, and Excel)

H.1.1 PROJECT MANAGER

It is required that the PM meet the qualifications of the Level II Project Manager labor category **(Basic Contract Section J, Attachment B)**. It is required that the PM have an active Project Management Institute (PMI) Project Management Professional (PMP®) or PMI Program Management Professional (PgMP®) Certification, or equivalent at the time of proposal submission.

It is desired that the PM has the following qualifications:

1. Experience in completing projects and leading or directing the work of others similar to the work described in Section C
2. Experience in completing complicated or complex tasks with limited guidance in a Cyberspace Operations environment

H.1.2 CYBERSPACE JOINT OPERATIONS PLANNER LEAD

The Cyberspace Joint Operation Planner Lead will serve as the technical lead for contractor personnel performing planning functions. It is required that the Cyberspace Joint Operation Planner Lead meet the qualifications of the Level III Cyberspace Joint Operation Planner **(Basic Contract Section J, Attachment B)**. In addition, it is required that the Cyberspace Joint Operation Planner Lead possesses a minimum of three years of experience with managing teams in an environment similar to the TO.

H.1.3 WEAPONS & CAPABILITIES LEAD

The Weapons & Capabilities Lead will serve as the technical lead for contractor personnel performing Fires, Media Malware Analysis, cyber capability analysis, IAVM, and fusion support functions, cyberspace capability management, and cyberspace joint munitions effectiveness support functions. It is required that the Weapons & Capabilities Lead posses the following qualifications:

1. A minimum of ten years of experience as a Cyberspace Analyst or experience in a similar functional area
2. A minimum of three years of experience in Cyber Fires and/or Cyber Targeting
3. DoD 8570 IAM Level III Certification
4. A minimum of three years of experience with managing teams in an environment similar to the TO

H.1.4 JOINT INFORMATION ENVIRONMENT OPERATIONS SPONSOR GROUP (JOSG) LEAD

The JOSG Lead will serve as a technical lead for those contractor personnel performing functions for the JOSG. It is required that the JOSG Lead possess the qualifications of the Level III Cyberspace Operations Engineer labor category **(Basic Contract Section J, Attachment B)**. It is also required that the JOSG Lead has the following qualifications:

1. Experience working with the JIE framework
2. A minimum of three years of experience with managing teams in an environment similar to the TO

H.1.5 CYBERSPACE OPERATIONS LEAD

The Cyberspace Operations Lead will serve as a technical lead for those contractor personnel performing DODIN Operations support functions. It is required that the Cyberspace Operations Lead meet the qualifications of the Level II Cyberspace Analyst **(Basic Contract Section J, Attachment B)**. It is required that the Cyberspace Operations Lead possess the following additional qualifications:

1. A minimum of three years of experience in DCO or Cyberspace Defense, previously known as Cyber Network Defense (CND)
2. A minimum of three years of experience with managing teams in an environment similar to the TO

H.1.6 KEY PERSONNEL SUBSTITUTION

The contractor shall not replace any personnel designated as Key Personnel without the written concurrence of the CO. Prior to utilizing other than personnel specified in proposals in response to a Solicitation, the contractor shall notify the Government CO and the FEDSIM COR of the existing Contract. This notification shall be no later than ten calendar days in advance of any proposed substitution and shall include justification (including resume(s) and labor category of proposed substitution(s)) in sufficient detail to permit evaluation of the impact on TO performance.

Substitute personnel qualifications shall be equal to, or greater than, those of the personnel being substituted. If the Government CO and the FEDSIM COR determine that a proposed substitute personnel is unacceptable, or that the reduction of effort would be so substantial as to impair the successful performance of the work under the Contract, the contractor may be subject to default action as prescribed by FAR 52.249-6 Termination (Cost Reimbursement).

H.2 GOVERNMENT-FURNISHED PROPERTY (GFP)

The Government will provide access to facilities, office space, supplies and services, to include workstations, computers, and phones. Access will be granted to classified and unclassified military local area network (LAN) services, LAN support, telephones, and reproduction facilities. If the contractor determines additional equipment is required, the contractor shall notify the Government, in writing, of the applicable information/equipment required to accomplish the requirements. The Government will provide access to relevant Government organizations, information, documentation, manuals, text briefs, and associated materials as required and available.

The contractor will be held accountable for the loss or destruction of Government property in the custody of contractor personnel, as documented by signed hand receipts, IAW the USCYBERCOM policies.

H.2.1 GOVERNMENT-FURNISHED INFORMATION (GFI)

The Government will provide workspace, computers, connectivity, and other resources required to accomplish the tasks outlined in this PWS for those contractor employees located at Government facilities. Contractors located at offsite facilities may receive GFE to perform the tasks defined in this PWS. Individual TOs will designate whether offsite contractor employees will receive GFE.

The Government will provide access to non-procurement-sensitive documentation, information on various weapon systems, program process and schedules, as well as intelligence and information pertaining to cyberspace activities ISO military information operations, related activities, and associated follow-on tasks to enable contractors to complete their assigned tasks.

Information will include reports, briefings and other related reference material. The Government will provide the contractor with timely information, to include access to both unclassified and classified Government information networks, and will facilitate contractor personnel interfaces with other DoD staff, service staff, and national agency offices as required to complete this effort.

H.7 SECURITY REQUIREMENTS

IAW DoD 5200.2-R, Section C2.1, all individuals shall be U.S. citizens. Personnel ineligible for these required security clearances are not permitted on this TO. All contractor personnel working on or managing this effort shall strictly adhere to USCYBERCOM, security regulations and procedures. All members of the contractor team (prime, sub-contractors, etc.) providing personnel, including supervisory personnel, to perform the work must comply with the applicable security clearance levels (facilities/personnel) based on the sensitivity of the task/work requiring a clearance.

Personnel must report to the CO and the FEDSIM COR all foreign travel, official and unofficial, in advance of the travel and agree to forego personal unofficial foreign travel when it is deemed by agency approving authorities to constitute a hazard to national security. The contractor shall report to the CO and the FEDSIM COR any of the following:

a. Continuing contact with citizens of a foreign country
b. Any arrest or court actions other than minor traffic violations
c. Any change in marital status. If, following employment, an employee marries (or cohabits with) a foreign national, termination of employment may be effected
d. Any bankruptcy, judgment, garnishment, lien, or other significant financial difficulties

Contractor personnel shall fully comply with USCYBERCOM in-processing and out-processing guidelines. At a minimum, the contractor shall:

a. Notify the TPOC of the employee's departure and his/her successful out-processing on the last day of work. Successful out-processing shall require, at a minimum, the turn-in/collection of all: (1) security badges; (2) smart cards and/or other comparable security devices; (3) GFE issued to the employee for performance of duties in accordance with local procedures. In additional, the employee shall receive security debrief.
b. Aggressively collect/recover and turn in security badges and devices, smart cards, and GFE to the TPOC or designate in any instance where the contractor employee fails to successfully out-process. Every effort shall be made to ensure these are recovered/turned in within 24 hours (one business day) of the departing employee's last day of work.
c. Coordinate changes in employment status with the TPOC affecting the accuracy of security badges and supporting records within 24 hours (one business day) of any such changes to ensure the appropriate devices are promptly reissued and/or collected.
d. Government-issued badges, identification cards, passes, vehicle registration media, and admittance controls are U.S. Government property and as such are to be accounted for, protected, and returned to the Government at the end of the contract period of performance or at any other time as required. When a contractor employee leaves the company, or ceases working on this contract, the employee shall adhere to all required USCYBERCOM out-processing procedures.

Situations may arise when fully cleared contractor personnel must perform opening and closing security duties unescorted in USCYBERCOM spaces. In accordance with USCYBERCOM security policy, contractors are authorized to perform these duties only with the TPOC or his/her designee's permission and if mission allows and/or requires it. In addition, fully cleared contractor personnel may be put on key lists with management/supervisor permission if mission allows and/or requires it. It is the responsibility of local Government management to establish and maintain internal procedures to protect the controlled items (this includes classified information) under their supervision. Access to secure areas should be limited to persons who are authorized to receive or have knowledge of the particular classified information or activities contained or conducted in that area and have a verified need-to know. It is also the responsibility for contractor personnel to follow these internal procedures to ensure continued compliance with USCYBERCOM Security policy.

With the exception of Government-approved courier duties, contractor personnel shall not remove classified information from the worksite, either physically or electronically, and under no

circumstances shall the contractor or its personnel allow any classified information to be stored at an off-site facility.

H.7.1 INFORMATION ASSURANCE

IAW Defense Federal Acquisition Regulation Supplement DFARS 239.7102-3, all contractors performing Information Assurance (IA)-related functions shall have the following minimum qualifications in accordance with DoD 8140.01 (replaces DoD 8570.01-M Information Assurance Workforce Improvement Program) guidelines commensurate to contractor's labor category and level,.

Contractor personnel shall ensure continuing adherence to accepted Government information technology policies and guidance applicable to this TOR. This includes public laws, executive orders, directives, regulations, manuals, standards, memorandums, and instructions.

H.7.1.1 SAFEGUARDING SENSITIVE DATA AND INFORMATION TECHNOLOGY RESOURCES

IAW FAR 39.105, this section is included in this Contract. This section applies to all users of sensitive data and IT resources, including awardees, contractors, subcontractors, lessors, suppliers, and manufacturers.

The following GSA policies must be followed. These policies can be found at: http://www.gsa.gov/directives

a. CIO P 2100.1 GSA Information Technology (IT) Security Policy
b. CIO P 2100.2B GSA Wireless Local Area Network (LAN) Security
c. CIO 2100.3B Mandatory Information Technology (IT) Security Training Requirement for Agency and contractor Employees with Significant Security Responsibilities
d. CIO 2104.1A GSA Information Technology IT General Rules of Behavior
e. CIO 2105.1 B GSA Section 508: Managing Electronic and Information Technology for Individuals with Disabilities
f. CIO 2106.1 GSA Social Media Policy
g. CIO 2107.1 Implementation of the Online Resource Reservation Software
h. CIO 2160.4 Provisioning of Information Technology (IT) Devices
i. CIO 2162.1 Digital Signatures
j. CIO P 2165.2 GSA Telecommunications Policy
k. CIO P 2180.1 GSA Rules of Behavior for Handling Personally Identifiable Information (PII)
l. CIO 2182.2 Mandatory Use of Personal Identity Verification (PIV) Credentials
m. CIO P 1878.2A Conducting Privacy Impact Assessments (PIAs) in GSA
n. CIO IL-13-01 Mobile Devices and Applications
o. CIO IL-14-03 Information Technology (IT) Integration Policy
p. HCO 9297.1 GSA Data Release Policy
q. HCO 9297.2B GSA Information Breach Notification Policy
r. ADM P 9732.1 D Suitability and Personnel Security

H.7.2 SECURITY CLEARANCES

The contractor (to include team members and subcontractors) shall be either a U.S.-owned firm or possess a favorable National Interest Determination if foreign owned. The contractor shall have a final TS Facility Clearance (FCL) from the DSS Facility Clearance Branch (FCB). The contractor shall have readily available access to DSS-certified work locations for performing classified work up to and including TS/ SCI at time of TO award. Individuals performing work under this TO shall be a U.S. citizen and comply with applicable program security requirements which will require TS personnel security clearances with SCI eligibility at time of award. The contractor shall comply with all appropriate security regulations in handling classified material and in publishing reports and other products.

Prior to being assigned to this TO, all contractor personnel shall possess a final TS/SCI eligible security clearance (granted full SCI eligibility by a U.S. Government Adjudication Authority within the past 60 months) and have not had a break in SCI access of more than 24 months during this period. Contractors shall have a Counterintelligence Scope Polygraph (CSP) examination conducted by a recognized U.S. Government polygraph entity within seven years (in scope) and Personnel Security Standards and Procedures Governing Eligibility for Access to SCI. Contractors shall have successfully undergone a Single Scope Background Investigation (SSBI) that is current (in scope) as defined by DoD 5200.2-R, DoD Manual 5105.21-V3, and ICD 704. The nature of this TO requires contractor personnel to possess a high degree of security awareness.

All contractor personal shall receive security indoctrination by USCYBERCOM and will be vetted and approved for access approval by the NSA Military Affairs Desk Office (MADO) prior to access to USCYBERCOM classified information, spaces, and IT systems and networks being granted. Contractors shall sign a USCYBERCOM specific Non-Disclosure Agreement (NDA) based on the tasks to be performed.

Contractor personnel shall keep the USCYBERCOM Office of Security, FEDSIM COR, and Counterintelligence apprised of any significant changes in personal status that could affect their eligibility for access to SCI.

H.8 ORGANIZATIONAL CONFLICT OF INTEREST AND NON-DISCLOSURE REQUIREMENTS

H.8.1 ORGANIZATIONAL CONFLICT OF INTEREST (OCI)

a. Determination. The Government has determined that this effort may result in an actual or potential conflict of interest, or may provide one or more offerors with the potential to attain an unfair competitive advantage. The nature of the conflict of interest may involve prime contractor, subcontractors of any tier, or contractor team arrangements maintaining contractual relationship or potential work with the USCYBERCOM. This includes program solutions pertaining to, but not limited to, the system, system components, specifications, work statements, interface resolutions, test requirements, test data, management of other contractors or design, evaluation services, and proprietary information. In accordance with FAR Subpart 9.5 the contractor shall immediately disclose this actual or potential OCI.

b. If any such conflict of interest is found to exist, the CO may (1) disqualify the offeror, or (2) determine that it is otherwise in the best interest of the U.S. to contract with the offeror and include the appropriate provisions to avoid, neutralize, mitigate, or waive such conflict in the contract awarded. After discussion with the offeror, the CO may determine that the actual conflict cannot be avoided, neutralized, mitigated or otherwise resolved to the satisfaction of the Government, and the offeror may be found ineligible for award.

c. Disclosure: The offeror hereby represents, to the best of its knowledge that:

___ (1) It is not aware of any facts which create any actual or potential organizational conflicts of interest relating to the award of this contract, or

___ (2) It has included information in its proposal, providing all current information bearing on the existence of any actual or potential organizational conflicts of interest, and has included a mitigation plan in accordance with paragraph (d) of this provision.

d. Mitigation. If an offeror with a potential or actual conflict of interest or unfair competitive advantage believes the conflict can be avoided, neutralized, or mitigated, the offeror shall submit a mitigation plan to the Government for review. Award of a contract where an actual or potential conflict of interest exists shall not occur before Government approval of the mitigation plan. If a mitigation plan is approved, the restrictions of this provision do not apply to the extent defined in the mitigation plan.

e. Other Relevant Information: In addition to the mitigation plan, the CO may require further relevant information from the offeror. The CO will use all information submitted by the offeror, and any other relevant information known to the General Services Administration (GSA), to determine whether an award to the offeror may take place, and whether the mitigation plan adequately neutralizes or mitigates the conflict.

f. Corporation Change. The successful offeror shall inform the CO within thirty calendar days of the effective date of any corporate mergers, acquisitions, and/or divestures that may affect this provision.

g. Flow-down. The contractor shall insert the substance of this clause in each subcontract of any tier that exceeds the simplified acquisition threshold.

H.8.2 NON-DISCLOSURE REQUIREMENTS

If the contractor acts on behalf of, or provides advice with respect to any phase of an agency procurement, as defined in FAR 3.104-4, then the contractor shall execute and submit a Corporate NDA Form **(Section J, Attachment F)** and ensure that all its personnel (to include subcontractors, teaming partners, and consultants) who will be personally and substantially involved in the performance of the TO:

a. Are listed on a signed Addendum to Corporate NDA Form **(Section J, Attachment F)** prior to the commencement of any work on the TO.

b. Are instructed in the FAR 3.104 requirements for disclosure, protection, and marking of contractor bid or proposal information, or source selection information

c. Are instructed in FAR Part 9 for third-party disclosures when acting in an advisory capacity

All proposed replacement contractor personnel also must be listed on a signed Addendum to Corporate NDA and be instructed in the requirements of FAR 3.104. Any information provided by contractors in the performance of this TO or obtained from the Government is only to be used in the performance of the Contract. The contractor shall put in place appropriate procedures for the protection of such information and shall be liable to the Government for any misuse or unauthorized disclosure of such information by its personnel, as defined above.

H.9 SECTION 508 COMPLIANCE REQUIREMENTS

Unless the Government invokes an exemption, all Electronic and Information Technology (EIT) products and services proposed shall fully comply with Section 508 of the Rehabilitation Act of 1973, per the 1998 Amendments, 29 United States Code (U.S.C.) 794d, and the Architectural and Transportation Barriers Compliance Board's Electronic and Information Technology Accessibility Standards at 36 Code of Federal Regulations (CFR) 1194. The contractor shall identify all EIT products and services provided, identify the technical standards applicable to all products and services provided, and state the degree of compliance with the applicable standards. Additionally, the contractor must clearly indicate where the information pertaining to Section 508 compliance can be found (e.g., Vendor's or other exact web page location). The contractor must ensure that the list is easily accessible by typical users beginning at TOA.

H.10 COST ACCOUNTING SYSTEM

The adequacy of the contractor's accounting system and its associated internal control system, as well as contractor compliance with the Cost Accounting Standards (CAS), affect the quality and validity of the contractor data upon which the Government must rely for its management oversight of the contractor and contract performance. The contractor's cost accounting system shall be adequate during the entire PoP and shall permit timely development of all necessary cost data in the form required by the contract.

H.11 PURCHASING SYSTEMS

The objective of a contractor purchasing system assessment is to evaluate the efficiency and effectiveness with which the contractor spends Government funds and complies with Government policy with subcontracting. The contractor is required to have an acceptable purchasing system in accordance with DFAR 252.244-7001.

Prior to the award of a TO, the CO will verify the validity of the contractor's purchasing system. Thereafter, the contractor is required to certify to the CO no later than 30 calendar days prior to the exercise of any options the validity of their purchasing system. Additionally, if reviews are conducted of the purchasing system after the exercise of the option, the contractor shall provide the results of the review to the CO within ten workdays from the date the results are known to the contractor.

H.12 TRAVEL

H.12.1 TRAVEL REGULATIONS

Personnel may be required to travel to CONUS or OCONUS locations for work-related conferences, meetings, training or exercises. Typically, contractor personnel will accompany

Government personnel on travel for no more than seven calendar days per occurrence. All travel shall be approved by the FEDSIM COR prior to occurrence.

Contractor costs for travel will be reimbursed at the limits set in the following regulations (see FAR 31.205-46):

a. Federal Travel Regulations (FTR) - prescribed by the GSA, for travel in the contiguous U.S.
b. Joint Travel Regulations (JTR), Volume 2, DoD Civilian Personnel, Appendix A - prescribed by the DoD, for travel in Alaska, Hawaii, and outlying areas of the U.S.
c. Department of State Standardized Regulations (DSSR) (Government Civilians, Foreign Areas), Section 925, "Maximum Travel Per Diem Allowances for Foreign Areas" - prescribed by the Department of State, for travel in areas not covered in the FTR or JTR

H.12.2 TRAVEL AUTHORIZATION REQUESTS

Before undertaking travel to any Government site or any other site in performance of this Contract, the contractor shall have this travel approved by, and coordinated with, the FEDSIM COR. Notification shall include, at a minimum, the number of persons in the party, traveler name, destination, duration of stay, purpose, and estimated cost. Prior to any long distance travel, the contractor shall prepare a Travel Authorization Request for Government review and approval. Long-distance travel will be reimbursed for cost of travel comparable with the JTR and DSSR.

Requests for travel approval shall:

a. Be prepared in a legible manner
b. Include a description of the travel proposed including a statement as to purpose
c. Be summarized by traveler
d. Identify the TO number
e. Identify the CLIN associated with the travel
f. Be submitted in advance of the travel with sufficient time to permit review and approval

The contractor shall use only the minimum number of travelers and rental cars needed to accomplish the task(s). Travel shall be scheduled during normal duty hours whenever possible.

H.13 TOOLS AND ODCs

The Government may require the contractor to purchase hardware, software, and related supplies critical and related to the services being acquired under the TO. Such requirements will be identified at the time a TOR is issued or may be identified during the course of a TO by the Government or the contractor. If the contractor initiates a purchase within the scope of this TO and the prime contractor has an approved purchasing system, the contractor shall submit to the FEDSIM COR a Request to Initiate Purchase (RIP) (**Section J.1, Attachment G**). If the prime contractor does not have an approved purchasing system, the contractor shall submit to the CO a Consent to Purchase (CTP). The RIP or CTP shall include the purpose, specific items, estimated cost, cost comparison, and rationale. The contractor shall not make any purchases without an approved RIP or CTP from the FEDSIM COR and without complying with the requirements of Section H.14, Commercial Software Agreements.

H.14 COMMERCIAL SOFTWARE AGREEMENTS

H.14.1 The Government understands that commercial software tools that may be purchased in furtherance of this TO as described in Section C.4 and as contemplated in the Tools and ODC CLINs in Section B may be subject to commercial agreements which may take a variety of forms, including without limitation licensing agreements, terms of service, maintenance agreements, and the like, whether existing in hard copy or in an electronic or online format such as "clickwrap" or "browsewrap" (collectively, "Software Agreements"). The parties acknowledge that FAR 12.212(a) requires the Government to procure such tools and their associated documentation under such Software Agreements to the extent such Software Agreements are consistent with Federal law.

H.14.2 IOT ensure that the Software Agreements are consistent with Federal law, the contractor shall not make any purchase contemplated in Section C.4 above without first securing the consent of the licensor of such software tools to amend the Software Agreements in accordance with the Amendment clause set forth in Section H.14.4 below. The contractor shall submit documentary evidence of such consent as part of its technical proposal.

H.14.3 The requirements of this Section H.14.3 apply only to those commercial software tools newly purchased under this TO; they do not apply to software furnished as GFI/GFE (if any). Further, they apply only to those Software Agreements that define the Government as the licensee or are intended to be transferred or assigned to the Government, with the Government becoming the licensee, at the end of this TO.

H.14.4 As used in the Amendment clause, the term "this Agreement" refers to each Software Agreement. The relevant definitions and the capitalization of terms (e.g., Licensee, Licensor, Software, Agreement) may be adjusted as necessary to match the nomenclature of the Software Agreement.

Amendment

For Federal Government Licensees, this Agreement is hereby amended as follows:

1. ***Dispute resolution and governing law****:* Any arbitration, mediation or similar dispute resolution provision in this Agreement is hereby deleted. This Agreement shall be governed by and interpreted and enforced in accordance with the laws of the United States of America, and dispute resolution shall take place in a forum, and within the time period, prescribed by applicable federal law. To the extent permitted by federal law and then only to the extent not preempted by federal law, the laws of the state specified in this Agreement (excluding its choice of law rules) will apply. No equitable or injunctive relief, and no shifting of legal fees or costs, may be sought against the Federal Government Licensee except as, and then only to the extent, specifically authorized by applicable federal statute.
2. ***Indemnification***: Any provisions in this Agreement requiring any Federal Government Licensee to indemnify any party are hereby deleted and shall not apply. Any provisions requiring the licensor to indemnify the Federal Government Licensee shall be revised to state that such indemnification, and the conduct and/or settlement of any applicable proceedings, shall be subject to 28 USC 516.

3. ***Changes in templates***: This Agreement shall apply in the version attached hereto. Subsequent updates to or changes in the licensor's standard commercial templates for such agreements shall not be binding on the Federal Government Licensee, except by prior express written agreement of both parties.
4. ***Fees, taxes, and payment:*** If the Software is licensed as part of a separate Government contract between the Federal Government Licensee and a prime contractor, the provisions of such contract regarding fees, taxes and payment shall supersede any provisions of this Agreement regarding same. Notwithstanding the foregoing: (a) express written agreement of the Federal Government Licensee shall be required prior to (i) any extension or renewal of this Agreement or the associated fees or (ii) any change in the fees; (b) late payments shall be governed by the Prompt Payment Act and the regulations at 5 CFR 1315; and (c) no cost of collection on delinquent invoices may be sought against the Federal Government Licensee except as, and then only to the extent, specifically authorized by applicable federal statute.
5. ***Assignment*****:** Licensor may not assign this Agreement or its rights or obligations thereunder, in whole or in part, except in accordance with the procedures set forth in FAR subparts 32.8 and/or 42.12, as applicable.
6. ***No waiver of liability or cause of action***: Any provision requiring the Federal Government Licensee to agree to waive or otherwise not to pursue any claim against the licensor it may otherwise have is hereby deleted. Without limiting the generality of the foregoing, the parties agree that nothing in this Agreement, including but not limited to the limitation of liability clauses, in any way grants the licensor a waiver from, release of, or limitation of liability pertaining to, any past, current or future violation of federal law and that no clause restricting users' statements shall be read to restrict the Federal Government Licensee's ability to pursue any course of action otherwise permitted by Federal law, regulation, or policy, including without limitation making public statements in connection with any suspension or debarment action.
7. ***Audit***: Any clauses in this Agreement allowing for an audit of the Federal Government Licensee's records or information systems, or verification of its compliance with this Agreement generally, shall be subject to the Federal Government Licensee's requirements pertaining to security matters, including without limitation clearances to be held and NDAs to be executed by auditors, badging or escorting requirements for access to premises, and other applicable requirements. Any overuse identified in an audit shall be referred to the prime contractor or the Federal Government Licensee's contracting officer (as applicable) for action. No audit costs may be sought against the Federal Government Licensee except as, and then only to the extent, specifically authorized by applicable federal statute.
8. ***Compliance with laws*****:** The parties acknowledge that the United States, as a sovereign, is subject to the laws of the United States. Nothing in this Agreement shall be interpreted to imply consent by any Federal Government Licensee to submit to the adjudicative or enforcement power of any regulatory, administrative, or judicial authority of, or the application of the laws of, another jurisdiction. Any provision inconsistent with applicable Federal law that is not

listed above is hereby deemed omitted from this Agreement to the extent of such inconsistency.

9. ***Third-party terms***: Any third-party licensing terms associated with third-party software components or products embedded in or otherwise provided with the Software shall be deemed amended in accordance with Sections 1-8 above.

H.15 INTELLECTUAL PROPERTY RIGHTS

The existence of any patent, patent application or other intellectual property right that encumbers any deliverable must be disclosed in writing on the cover letter that accompanies the delivery. If no such disclosures are provided, the data rights provisions in DFAR 252.227-7014 apply.

The Software Agreements referenced in section H.14, amended as contemplated therein, shall be deemed to constitute such disclosure with regard to their associated commercial software tools and shall prevail over any inconsistent provision in FAR 52.227-14 to the extent of such inconsistency.

H.16 CONTRACTOR IDENTIFICATION

As stated in 48 CFR 211.106, Purchase Descriptions for Service Contracts, contractor personnel shall identify themselves as contractor personnel by introducing themselves or being introduced as contractor personnel and by displaying distinguishing badges or other visible identification for meetings with Government personnel. Contractor personnel shall appropriately identify themselves as contractor employees in telephone conversations and in formal and informal written correspondence.

H.17 REQUIRED INSURANCE (IAW FAR 28.307)

IAW FAR 28.307, "the contractor shall, at its own expense, procure and thereafter maintain the following kinds of insurance with respect to performance under the contract."

a. Workmen's Compensation and Employers Liability Insurance as required by law except that if this contract is to be performed in a State which does not require or permit private insurance, then compliance with the statutory or administrative requirements in any such State will be satisfactory. The required Workmen's Compensation insurance shall extend to cover employer's liability for accidental bodily injury or death and for occupational disease with a minimum liability limit of $100,000.

b. General Liability Insurance. Bodily injury liability insurance, in the minimum limits of $500,000 per occurrence, shall be required on the comprehensive form of policy.

c. Automobile Liability Insurance. This insurance shall be required on the comprehensive form of policy and shall provide bodily injury liability and property damage liability covering the operation of all automobiles used in connection with the performance of the contract. At least, the minimum limits of $200,000 per person and $500,000 per occurrence for bodily injury and $20,000 per occurrence for property damage shall be required.

H.18 CONTRACTOR WORK PERIOD AND FACILITY ACCESS

The TPOC determines core working hours. Core work hours will vary between each of the task areas. If contractors are required to work extended hours, contractors are expected to adjust their

hours before and after these extended hour periods to stay within the proposed total number of hours. Facility closures as a result of inclement weather, potentially hazardous conditions, or other special circumstances shall be expected. During those periods, personnel shall not be provided access to facilities unless they are designated as emergency or essential personnel. The TPOC are the only individuals who can designate personnel as emergency or essential unless otherwise specified within the contract. The TO PM shall provide the TPOC or his/her designee daily accountability of personnel supporting this contract.

During Government Federal Holidays, down days, or inclement weather, certain facilities will be closed or determined to have restricted use. During those times, contractors will not be permitted to work in those certain Government facilities or charge the Government. In the event of operational driven support during those times, the contractor shall obtain written authorization by the FEDSIM COR prior to time of need. If the FEDSIM COR does authorize the contractor to work at an off-site location, this location shall be an approved corporate facility in which the contractor supervisor/team lead shall be present to ensure all work being accomplished is directly attributable to its TO. In addition, the FEDSIM COR must submit, in writing, authorization for the contractor to work at their corporate off-site location to the CO prior to the need. A home office is never an approved off-site work location. FEDSIM CORs shall allow contractors to adjust their schedules to compensate for missed times and have the option to work extended workdays, if desired.

H.19 CONTRACTOR IDENTIFICATION

As stated in 48 CFR 211.106, Purchase Descriptions for Service Contracts, contractor personnel shall identify themselves as contractor personnel by introducing themselves or being introduced as contractor personnel and by displaying distinguishing badges or other visible identification for meetings with Government personnel. Contractor personnel shall appropriately identify themselves as contractor employees in telephone conversations and in formal and informal written correspondence.

NOTE: Section I of the Contractor's MA IDIQ is applicable to this TO and is hereby incorporated by reference. In addition, the following applies:

I.1 FAR 52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)

This TO incorporates one or more clauses by reference with the same force and effect as if they were given in full text. Upon request, the CO will make their full text available. Also, the full text of a provision may be accessed electronically at the FAR website:

http://www.acquisition.gov/far/

Clause No	Clause Title	Date
52.203-13	Contractor Code of Business Ethics and Conduct	(Apr 2010)
52.203-14	Display of Hotline Posters (http://www.dodig.mil/Hotline/posters.cfm)	(Dec 2007)
52.204-2	Security Requirements	(Aug 1996)
52.204-9	Personal Identity Verification of Contractor Personnel	(Jan 2011)
52.204-10	Reporting Executive Compensation and First Tier Subcontract Awards	(Jul 2013)
52.215-21	Requirements for Cost or Pricing Data or Information Other than Cost or Pricing Data – Modifications	(Oct 2010)
52.216-8	Fixed Fee	(Jun 2011)
52.219-8	Utilization of Small Business Concerns	(Oct 2014)
52.219-9	Small Business Subcontracting Plan	(Oct 2014)
52.223-15	Energy Efficiency in Energy Consuming Products	(Dec 2007)
52.223-16	Acquisition of EPEAT-Registered Personal Computer Products	(Jun 2014)
52.224-1	Privacy Act Notification	(Apr 1984)
52.224-2	Privacy Act	(Apr 1984)
52.227-14	Rights in Data – General	(May 2014)
52.227-14	Rights In Data – General Alternate II or III	(May 2014)

Clause No	Clause Title	Date
52.227-15	Representation of Limited Rights Data and Restricted Computer Software	(Dec 2007)
52.227-17	Rights In Data Special Works	(Dec 2007)
52.227-21	Technical Data Declaration Revision and Withholding of Payment – Major Systems	(May 2014)
52.232-18	Availability of Funds	(Apr 1984)
52.232-20	Limitation of Cost	(Apr 1984)
52.232-22	Limitation of Funds	(Apr 1984)
52.232-99	Providing Accelerated Payment to Small Business Subcontractors (Deviation)	(Dec 2013)
52.239-1	Privacy or Security Safeguards	(Aug 1996)
52.244-6	Subcontracts for Commercial Items	(Apr 2015)
52.251-1	Government Supply Sources	(Apr 2012)

I.2 GENERAL SERVICES ADMINISTRATION ACQUISITION MANUAL (GSAM), CLAUSES INCORPORATED BY REFERENCE

The full text of a provision may be accessed electronically at the GSAM website:

https://www.acquisition.gov/gsam/gsam.html

Clause No	Clause Title	Date
552.204-9	Personal Identity Verification Requirements	(Oct 2012)
552.232-25	Prompt Payment	(Nov 2009)
552.236-75	Use of Premises	(Apr 1984)
552.239-70	Information Technology Security Plan and Security Authorization	(Jun 2011)
552.239-71	Security Requirements for Unclassified Information Technology Resources	(Jan 2012)

I.1.1 CLAUSES INCORPORATED BY FULL TEXT

52.217-8 OPTION TO EXTEND SERVICES (NOV 1999)

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

(End of clause)

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

a. The Government may extend the term of this contract by written notice to the Contractor within 30 days; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 60 days before the contract expires. The preliminary notice does not commit the Government to an extension.
b. If the Government exercises this option, the extended contract shall be considered to include this option clause.
c. The total duration of this contract, including the exercise of any options under this clause, shall not exceed 66 months.

(End of clause)

I.3 DEFENSE FEDERAL ACQUISITION REGULATION SUPPLEMENTS (DFARS) CLAUSES INCORPORATED BY REFERENCE

The full text of a provision may be accessed electronically at the Defense Procurement website:

www.acq.osd.mil/dpap/dars/dfarspgi/current/index.html

Clause No	Clause Title	Date
252.204-7004	Alternate A, Central Contractor Registration	(Sep 2007)
252.211-7003	Item Identification and Valuation	(Jun 2013)
252.227-7013	Rights in Technical Data - Noncommercial Items	(Feb 2014)
252.227-7014	Rights in Noncommercial Computer Software and Noncommercial Computer Software Documentation	(Feb 2014)
252.227-7015	Technical Data-Commercial Items	(Feb 2014)
252.227-7016	Rights in Bid or Proposal Information	(Jan 2011)

Clause No	Clause Title	Date
252.227-7019	Validation of Asserted Restrictions - Computer Software	(Jun 1995)
252.227-7028	Technical Data or Computer Software Previously Delivered to the Government	(Jun 1995)
252.232-7007	Limitation of Government's Obligation	(Apr 2014)
252.239-7999	Cloud Computing Services (DEVIATION 2015-O0011)	(Feb 2015)
252.246-7001	Warranty of Data	(Mar 2014)

I.4 DEPARTMENT OF HOMELAND SECURITY (DHS) ACQUISITION REGULATION SUPPLEMENTS (HSAR) CLAUSES INCORPORATED BY REFERENCE

The full text of a provision may be accessed electronically at HSAR website:

www.dhs.gov/publication/homeland-security-acquisition-regulation-deviations/

Clause No	Clause Title	Date
HSAR Class Deviation 15-01	Safeguarding of Sensitive Information	(Mar 2015)

SECTION J – LIST OF ATTACHMENTS

NOTE: Section J of the Contractor's MA IDIQ is applicable to this TO and is hereby incorporated by reference. In addition, the following applies:

The following attachments are attached, either in full text or electronically..

J.1 LIST OF ATTACHMENTS

Attachment	Title
A	Incremental Funding Chart (Attached at award)
B	COR Appointment Letter (Attached at award)
C	Monthly Status Report (Attached at award)
D	Deliverable Acceptance-Rejection Report (Attached at award)
E	Problem Notification Report (PNR) Template (Attached at award)
F	Corporate NDA Form (Attached at award)
G	Request to Initiate Purchase Template (Attached at award)
H	Travel Request (Attached at award)
I	Acronym List

ATTACHMENT I -
ACRONYM LIST

ACAS	Assured Compliance Assessment Solution
AOR	Area of Responsibility
ASSIST	Assisted Services Shared Information System
B2C2WG	Boards, Bureaus, Centers, Cells and Working Groups
BPR	Business Process Re-engineering
C2	Command and Control
C3PO	Cyber Command and Control Portal for Operations
C4IT	Command, Control, Communications, Computers & Information Technology
CAPCO	Controlled Access Program Coordination Office
CAS	Cost Accounting Standards
CC/S/A/FA	Combatant Command/Service/Agency/Field Activity
CCIR	Commander's Critical Information Requirements
CCMD	Combatant Command
CCR	Cyberspace Capability Registry
CCRI	Command Cyber Readiness Inspection
CDA	Congressionally Directed Actions
CDC	Cleared Defense Contractor
CDS	Cross Domain Solution
CERF	Cyber Effects Request Form
CERT	Computer Emergency Response Team
CFR	Code of Federal Regulations
CI	Counter-Intelligence
CIO	Chief Information Officer
CJCSM	Commander Joint Chiefs of Staff Manual
CKO	Chief Knowledge Officer
CKT	Cyber Key Terrain
CLIN	Contract Line Item Number
CMF	Cyber Mission Force
CMRS	Continuous Monitoring Risk Score
CND	Cyber Network Defense
CNODB	Cyber Network Operations Database
CO	Contracting Officer

COA	Courses of Action
COCB	Cyber Operational Capabilities Board
CONOPS	Concept of Operations
CONUS	Continental United States
COOP	Continuity of Operations Plan
COR	Contracting Officer's Representative
CPFF	Cost-Plus-Fixed-Fee
CRC	Cyber Requirements Cell
CRIB	USCYBERCOM Requirements and Investment Board
CS	Control Systems
CSP	Counterintelligence Scope Polygraph (CSP)
CTC	Cyber Tasking Cycle
CTO	Cyberspace Tasking Order
CTP	Consent to Purchase
DCAA	Defense Contract Audit Agency
DCO	Defensive Cyberspace Operations
DFARS	Defense Federal Acquisition Regulation Supplement
DHS	Department of Homeland Security
DIB	Defense Industrial Base
DISA	Defense Information Systems Agency
DNS	Domain Name System
DoD	Department of Defense
DODIN	Department of Defense Information Network
DSS	Defense Security Service
DSSR	Department of State Standardized Regulations (DSSR)
EEFI	Essential Elements of Friendly Information
EIT	Electronic and Information Technology
EResM	Evaluation Response Message
EReqM	Evaluation Request Message
ERP	Enterprise Resource Planning
FAL	Functional Area Lead
FCB	Facility Clearance Branch
FCL	Facility Clearance
FEDSIM	Federal System and Integration Management Center
FOC	Full Operational Capability

FOIA	Freedom of Information Act
FTR	Federal Travel Regulation
GFE	Government-Furnished Equipment
GFI	Government-Furnished Information
GFP	Government-Furnished Property
GPS	Global Positioning System
GSAM	General Services Administration Acquisition Manual
HBSS	Host Based Security System
HIDS	Host Intrusion Detection System
IA	Information Assurance
IAVA	Information Assurance Vulnerability Alerts
IAVB	Information Assurance Vulnerability Bulletins
IAVM	Information Assurance Vulnerability Management
IAW	In Accordance With
IC	Intelligence Community
ICRWG	Integrated Capabilities Requirements Working Group
IDIQ	Indefinite Delivery Indefinite Quantity
IDM	Internal Defensive Measures
IOC	Initial Operational Capability
IOT	In Order To
ISO	In Support Of
IT	Information Technology
J3	Directorate of Cyberspace Operations
J6	Command, Control, Communications, Computers Information Technology (C4IT) Directorate
J7	Joint Exercises and Training Directorate
JACWC	Joint Advanced Cyber Warfare Course
JCAAS	Joint Capability and Analysis Assessment System
JELC	Joint Event Lifecycle
JFHQ	Joint Force Headquarters
JIACG	Joint Interagency Coordination Group
JID	Joint Indicator Database
JIE	Joint Information Environment
JIMS	Joint Incident Management System
JMC	Joint Malware Catalog

JMEM	Joint Munitions Effectiveness Manual
JOC	Joint Operations Center
JOPP	Joint Operational Planning Process
JOSG	Joint Information Environment Operations Sponsor Group
JQRR	Joint Quarterly Readiness Review
JTCB	Joint Targeting Coordination Board
JTCG	Joint Targeting Coordination Group
JTF	Joint Travel Regulation
JTSO	Joint Information Environment Technical Synchronization Office
JTWG	Joint Targeting Working Group
LAN	Local Area Network
LE	Law Enforcement
MA	Multiple Award
MADO	Military Affairs Desk Office
MCOP	Master Cyber Operations Plan
MD5	Message Digest 5
ME	Munitions Effectiveness
MIDB	Modernized Integrated Database
MMA	Media, Malware, and Analysis
MNS	Mission Needs Statements
MOE	Measure of Effectiveness
MOP	Measure of Performance
MS	Microsoft
MSR	Monthly Status Report
NAI	Named Areas of Interest
NDA	Non-Disclosure Agreement
NIDS	Network Intrusion Detection System
NISP	National Industrial Security Program
NIST	National Institute of Standards and Technology
NLT	No Later Than
NSA	National Security Agency
NTE	Not to Exceed
OCI	Organizational Conflict of Interest
OCO	Offensive Cyberspace Operations
OCONUS	Outside the Continental United States

ODC	Other Direct Cost
OPG	Operational Planning Groups
OPLAN	Operations Plan
OPORD	Operations Order
OPT	Operational Planning Teams
ORSA	Operations Research/System Analysis
OSD	Office of the Secretary of Defense
PCC	Planning and Coordination Cell
PDF	Portable Document Format
PgMP®	Program Management Professional
PII	Personally Identifiable Information
PIR	Priority Intelligence Requirements
PIT	Platform Information Technology
PIV	Personal Identity Verification
PM	Project Manager
PMI	Project Management Institute
PMP®	Project Management Professional
PMP	Project Management Plan
PNR	Problem Notification Report
PNT	Positioning, Navigation, and Timing
POA&M	Plan of Action and Milestones
PoP	Period of Performance
PWS	Performance Work Statement
QCP	Quality Control Plan
QFR	Questions for the Record
RAP-CO	Review and Approval Process for Cyberspace Operations
RFI	Request for Information
RIP	Request to Initiate Purchase
ROC	Rehearsal of Concept
SAP	Special Access Program
SATCOM	Satellite Communications
SCI	Sensitive Compartmented Information
SFE	Space Force Enhancements
SIP	Security In-Process
SLA	Service Level Agreement

SME	Subject Matter Expert
SOP	Standard Operating Procedures
SSBI	Single Scope Background Investigation
SSO	Staff Security Office
STO	Special Technical Operations
TASKORD	Tasking Order
TMF	Threat Mitigation Framework
TO	Task Order
TOA	Task Order Award
TOR	Task Order Request
TPOC	Technical Point of Contact
TS	Top Secret
TTP	Tactics, Techniques, and Procedures
TTX	Tabletop Exercise
UCAP	Unified Cyber Analytics Portal
U.S.	United States
U.S.C.	United States Code
USCYBERCOM	United States Cyber Command
USSTRATCOM	United States Strategic Command
WBS	Work Breakdown Structure
WMS	Workflow Management System

SECTION K – REPRESENTATIONS, CERTIFICATIONS, AND OTHER STATEMENTS OF OFFERORS OR RESPONDENTS

NOTE: Section K of the Contractor's MA IDIQ is applicable to this TO and is hereby incorporated by reference.

This page intentionally left blank.

This page intentionally left blank.

This page intentionally left blank.