CAMPAIGN PLAN AND
CAPABILITIES DEVELOPMENT (CP&CD)
United States Transportation Command (USTRANSCOM)
PERFORMANCE WORK STATEMENT (PWS)
10 November 2022

1.0. DESCRIPTION OF SERVICES

1.1. Background The United States Transportation Command (USTRANSCOM) provides global air, land, and sea transportation for the Department of Defense (DOD), both in times of peace and war, through its Transportation Component Commands (TCCs): Surface Deployment and Distribution Command (SDDC), Military Sealift Command (MSC), Air Mobility Command (AMC), and Joint Enabling Capabilities Command (JECC). USTRANSCOM provides synchronized transportation, distribution, and sustainment, which makes possible projecting and maintaining national power where needed with the greatest speed and agility, the highest efficiency, and most reliable level of trust and accuracy.

The focal point for USTRANSCOM's campaign planning efforts are the DOD Functional Campaign Plan for Global Deployment and Distribution (FCP-GDD) and USTRANSCOM's Combatant Command Campaign Plan (USTRANSCOM CCP). The FCP-GDD operationalizes the USTRANSCOM Commanding General's (CDRUSTRANSCOM) strategy for Joint Deployment and Distribution Enterprise (JDDE) Partners. The plan seeks to address the challenge of global deployment and distribution, by designating JDDE desired "Effects", on behalf of the Chairman of the Joint Chiefs of Staff (CJCS) and the Secretary of Defense's (SEC DEF), for DOD's Global Integration Efforts. The USTRANSCOM CCP operationalizes the USTRANSCOM Commanding General's strategy for USTRANSCOM Headquarters and its Component Commands. The plan seeks to achieve CDRUSTRANSCOM's initiatives, Global Campaign Plans' and Functional Campaign Plans' effects, assigning "Tasks" internal to USTRANSCOM.

Capabilities Development is the command focal point for integrating several enterprise managements processes to produce new capabilities for Logistics, Strategic Mobility, Distribution, and the Defense Transportation System (DTS) to include Joint Capability Integration Development System (JCIDS), Integrated Priority List (IPL), Capability Gap Assessment (CGA), and Program Budget Review Issue Nomination Development.

1.2. Scope: CDRUSTRANSCOM is responsible for JDDE planning and operations across all domains and will collaborate with the Combatant Commands (CCMD), the Services, and, as directed, U.S. government agencies and commercial entities. The purpose of this contract is to provide strategic functional expertise enabling the USTRANSCOM Strategic Plans, Policy & Logistics Directorate (TCJ5/J4) to enhance the JDDE and enhance capabilities in support of the warfighter. This support includes multimodal deployment, distribution (sealift/airlift/ground movements), and supply chain operations; development, staffing and implementation of global campaign, functional campaign and distribution plans across the JDDE. A thorough understanding of the DOD campaign planning construct and contingency or campaign planning experience at the Combatant Command (CCMD) or Service-level is required. The services

provided within the scope of this contract are considered Covered Defense Information (CDI) as defined in Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012 Safeguarding CDI and Cyber Incident Reporting.

Support is required in the following Task Areas:

Task Area 1: Task Order Management
Task Area 2: Joint Deployment and Distribution Enterprise (JDDE) Campaign Planning
Task Area 3: Task Area 3: Capability Development

1.3. Applicable Documents:

The most current version of the following reference documents is applicable to this PWS:

- Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 5123.01I series, Charter of the Joint Requirements Oversight Council
- CJCSI 3100.01E Joint Strategic Planning System
- DOD Functional Campaign Plan for Global Deployment and Distribution (FCP-GDD) Guidance for Employment of the Force (GEF)
- Joint Capabilities Integration and Development System (JCIDS) Manual
- Joint Publication 5-0 Joint Planning
- Joint Strategic Campaign Plan
- National Defense Strategy (NDS)
- National Military Strategy (NMS)
- National Security Strategy (NSS)
- Unified Command Plan (UCP)
- USTRANSCOM Instruction 63-10, Acquisition Program Lifecycle Management
- USTRANSCOM Instruction 90-6, Corporate Governance Process
- USTRANSCOM Instruction 90-13, Mission Area Management
- USTRANSCOM Instruction 3900.04, Joint Capabilities Integration & Development System
- USTRANSCOM Combatant Command Campaign Plan
- *Other Contingency Planning Guidance as directed in performance of tasks

Websites:
https://jrockmdsbpm.js.smil.mil

1.4. Requirements

1.4.1. Task Area 1: Task Order Management
This task consists of contractor activities relating to the overall contract administration and management of the entire PWS. The contractor shall provide program management of contractor personnel performing tasks in this order. The contractor shall designate a principal point of contact for technical issues. The contractor shall provide support to the Contracting Officer Representatives (CORs) by preparing documents such as monthly status reports, in process reviews briefings, and general meeting minutes related to the status of the performance of this

task order. Other deliverables - information briefings and informational point papers - shall be prepared based on specific problem statements or monthly reports. All decisions regarding Government requirements or Government actions will be made by Government personnel. The Contractor shall submit required evaluations and recommendations to the COR and/or Contracting Officer (CO) for further action as appropriate. The Contractor shall coordinate with the Government to ensure that all activities are well synchronized and integrated with other USTRANSCOM and distribution management efforts. All reports, studies, or policies identified in the PWS shall be prepared and submitted for Government approval or acceptance. All functions and activities shall be task driven and work performed shall be in accordance with all applicable regulations and guidelines.

1.4.1.1. Monthly Status Report (MSR)
The Contractor shall submit a MSR within the first five business days of each month to report activity for the previous month. The MSR shall outline the current travel funding status, a brief synopsis of efforts completed, the status of efforts in progress, deliverables provided, and a list of seminars, conferences and trips conducted/attended during the reporting period. The report shall also describe the objectives to be accomplished during the next reporting period, an overall evaluation of the contract to date, and any issues, problem areas, and items that require Government action. The final MSR is due on the last day of the contract.

1.4.1.2. In-Process Reviews (IPRs)
The contractor shall support a quarterly IPR review with the COR to discuss status, issues, events, and current tasks. The contractor shall arrange the quarterly in-person meeting at a time agreed upon with the COR within 30 days of the end of the quarter. The IPR will be used to provide ensuing government decisions or guidance necessary to contractor performance. The contractor shall prepare a pdf document containing a summary of key accomplishments and activities related to each Task. The IPR Summary is due 5 business days prior to the IPR. The IPR review meeting is preferred to be in-person but may be accomplished via teleconference as circumstances allow. The decision of in-person or via teleconference shall be made by the COR.

1.4.1.3. Trip Reports
Within five (5) business days of completion of travel, the Contractor shall submit a trip report to include the following details: purpose, location and length of trip, travelers, and individuals contacted during trip, synopsis of all discussions, future actions identified, decisions made, or issues of concern arising during trip.

1.4.1.4. Employment Status Report
The Contractor shall provide an employee status report containing names and labor categories of personnel supporting each Task Area. The contractor shall provide the report within twenty-five (25) business days after task order award. Any changes in personnel shall be submitted in writing within five (5) business days after such changes occur.

1.4.2. Task Area 2: Joint Deployment and Distribution Enterprise (JDDE) Campaign Planning. The contractor shall support JDDE Campaign Planning directed by commander USTRANSCOM and higher headquarters. This task requires expertise in the following areas:

- Multimodal deployment, distribution (sealift/airlift/ground movements)

- Supply chain operations; development, staffing and implementation of global campaign, functional campaign and distribution plans across the JDDE
- DOD campaign planning construct and contingency or campaign planning experience at the Combatant Command (CCMD) or Service-level
- Strategic guidance contained in the Joint Strategic Campaign Plan (JSCP), Guidance for Employment of the Force (GEF), and the Unified Command Plan (UCP) and how they influence Global Campaign Plans (GCP), Combatant Command Campaign Plans (CCP), Functional Campaign Plans (FCP), Theater Distribution Plans (TDP) and Theater Posture Plans (TPPs)

1.4.2.1. Analytical and Technical Writing Support

The contractor shall support revisions to Campaign Plan documents and associated supporting staff processes, revisions due NLT 5 business days after receipt of Government comments. The contractor shall provide the following support:

- Assist the government in the design, layout and editing of the campaign plans, associated annexes and appendices, Campaign Plan Assessment (CPA), Global and Functional Campaign Plan Assessments, associated annexes and appendices, Command Strategy Forum (CSF) briefing materials and minutes, Joint Staff Action Packages (JSAPs), white papers, point papers and other campaign plan documents using standard desktop publishing tools/word processors
- Assess documents for gaps and inconsistencies, provide comments/recommendations during the revision of documents, and assist in the refinement and finalization of documents,
- Prepare presentations to explain the logic and content of campaign clan publications to USTRANSCOM personnel, JDDE partners, and other personnel (e.g., OSD, Joint Staff, and CCMDs),
- Attend associated working group meetings, research, draft, and provide supporting papers and briefings on strategic distribution issues,
- Assist the government in related Task Management Tool (TMT) tasking, point papers and presentations including preparing graphics and other audiovisual materials.

All Full Time Equivalent (FTE) supporting this task shall have a Top Secret/Sensitive Compartmentalized Information (SCI) clearance. The contractor support for this task shall be onsite. However, the contractor may process unclassified and classified data at company site if they already have a government approved facility/systems for handling/storing classified information in order to provide the support requested above.

1.4.2.2. Knowledge and Data Management

The contractor shall provide knowledge and data management support for campaign plan activities and supporting staff processes. Contractor support in this task areas requires expert experience with common data analysis software and programs (i.e., spreadsheets), briefing and writing capabilities appropriate for senior level audiences, proficiency using Microsoft Office suite/SharePoint functions, and familiarity with Command and Control of the Information Environment (C2IE) system. The contractor shall provide the following support:

- Manage Non-classified Internet Protocol Router Network (NIPRNet) and Secret Internet Protocol Router Network (SIPRNet) collaboration web sites, such as IntelShare and C2IE, in support of campaign planning and related tasks
- Collect, collate, and distribute data as appropriate to aid campaign planning and assessment efforts
- Develop and maintain a plan for the creation and storage of data on network drives separate from Intelshare websites
- Develop and provide a storage structure to include file naming conventions and folder storage structure using government provided share drive resources
- Develop and maintain a standard minute's format and archival process
- Distribute collected and collated data in support of campaign plans and the assessment process
- Archive products, minutes, and briefs to include meeting minutes from the monthly Planners' forum, monthly CSFs, Campaign Planning Joint Planning Groups (JPG), and other products as directed by the government
- Maintain NIPR and SIPR contact rosters for the JDDE community of interest (COI), and other contact lists as defined by the government
- Track and report TMT tasking, document review, and staffing,

All FTE supporting this task shall have a Secret clearance. The contractor support for this task shall be onsite. However, the contractor may process unclassified and classified data at company site if they already have a government approved facility/systems for handling/storing classified information in order to provide the support requested above.

1.4.2.3 Campaign Planning Support

The contractor shall assist in shaping and developing the Joint Deployment and Distribution Enterprise (JDDE) through the execution of campaign plans, to include maintenance and revision of the plan, and determining the impact of strategic guidance on USTRANSCOM's ability to execute campaign plans. The contractor shall provide the following support:

- Facilitate sessions with USTRANSCOM, Defense Agencies, Services, CCMDs, OSD and the Joint Staff including, as required, senior officers or action officers, and other JDDE stakeholders as needed to support the JDDC's guidance, provide read ahead materials as appropriate
- Author, edit, and recommend change to strategic guidance, joint publications, and other guidance in accordance with the specified review cycle
- Author, edit, and recommend changes to the FCP-GDD campaign base plan, annexes, and associated attachments tabs as required in accordance with Strategic Guidance, Joint Publications, Joint Operation Planning, Chairman of the Joint Chiefs of Staff Instructions and Manuals, and CDRUSTRANSCOM guidance,
- Review supporting and complimentary plans (e.g., NSS, UCP, CPG, NDS, GEF, NMS, JSCP, JSCP LOGSUP, GCP, CCMD Campaign Plans, FCP, TDP and TPPs), directives, and doctrine in accordance with government criteria to ensure alignment with all DOD Plans
- Support TCJ5-GP in collaborative JDDC process activities (e.g., conferences, seminars, VTCs, DCOs, staff coordination, etc.)

- Conduct coordination activities by providing support to Supported Command planners, their component planners, and USTRANSCOM component planners, Joint Staff, DLA and other supporting agency participants in preparation for and during seminars
- Provide multimodal, distribution, transportation and logistics planning, subject matter expertise for USTRANSCOM and TCJ5/J4 at meetings, seminars and conferences to discuss the USTRANSCOM JDDE responsibilities, the campaign planning process and other issues affecting deployment and distribution coordination across the DOD
- Attend events as representation for TCJ5/J4, to include but not limited to National Defense Transportation Association (NDTA), Commander's Call, Directorate Calls, war-games, and exercises, as directed by the government
- Prepare Line of Effort (LOE) reporting using the format provided by the government in support of the assessment process
- Assist LOE leads in determining the alignment of gaps and seams in the JDDE to intermediate objectives found in FCP-GDD and USTRANSCOM CCP
- Prepare and consolidate additional briefing material as requested by TCCS or other members of the CSF in the format provided by the government
- Submit detailed CSF meeting minutes no later than five business days after the completion of a CSF. CSF meeting minutes shall document the content of the CSF, to include tasks assigned, OPRs for each task, and results of CSF voting
- Support the creation of any briefs and TMTs required of the Campaign Planning team as a result of proceedings at the CSF
- Collect and adjudicate FCP-GDD campaign plans comments and requests for revision from USTRANSCOM and other JDDE partners
- Assist the government in preparation of and delivery of FCP-GDD campaign plan training, integrated planning teams, and IPR
- Provide trip reports/after action reports for each FCP-GDD campaign plan staff visit, seminar, conferences, and IPRs
- Assist the government with related TMT tasking, point papers, and presentations

All FTE supporting this task shall have a Top Secret/Sensitive Compartmentalized Information (SCI) clearance. The contractor support for this task shall be onsite. However, the contractor may process unclassified and classified data at company site if they already have a government approved facility/systems for handling/storing classified information in order to provide the support requested above.

1.4.2.4 Assessment Support

The contractor shall support USTRANSCOM CCP assessment, the Global and Functional Campaign Plans' Assessment, the Annual Joint Assessment, and other operations assessments, as directed by commander USTRANSCOM or higher headquarters. This task requires strong critical thinking capabilities, excellent briefing and writing skills, and experience with quantitative and qualitative analytic techniques. The contractor shall provide the following support:

- Collect information from internal and external sources, as identified by the government
- Aggregate and analyze the collected information to develop trend analysis

- Conduct monthly and annual assessments for each USTRANSCOM CCP LOE based on the information collected, aggregated, and analyzed using the process outlined by the government
- Prepare CSF assessment briefings in support of monthly CSF
- Interpret assessment results and provide recommendations to the government
- Prepare campaign plan assessments, Annual Joint Assessment (AJA), and Global Distribution Assessment (GDA) reports and briefings as directed by the government
- Provide briefing materials for the campaign plan assessments, AJA, and GDA, include findings and recommendations
- Assist the government in developing campaign plan assessments, AJA, and GDA products, processes, frameworks, and effectiveness measures
- Assist with Task Management Tool (TMT) tasking, document review and staffing, point papers, and presentations including preparing graphics and other audiovisual materials
- Support additional assessments, as directed by the government

FTE's supporting this task shall have a Top Secret/Sensitive Compartmentalized Information (SCI) clearance. The contractor support for this task shall be onsite. However, the contractor may process unclassified and classified data at company site if he/she already have a government approved facility/systems for handling/storing classified information in order to provide the support requested above.

1.4.2.4.1 Global and Functional Campaign Plan (GCP) Assessment Support

The contractor shall support Global Campaign Plan Assessments as directed by commander USTRANSCOM and higher headquarters. This task requires knowledge and experience with campaign plans, strategic documents, and excellent verbal and written communication skills. The contractor shall:

- Coordinate with the Joint Staff, CCMDs, and designated coordinating authorities on the assessment of global and functional campaign plans
- Provide comments on interactions with Joint Staff, CCMDs, and designated coordinating authorities on the assessment of GCPs
- Identify, evaluate, and recommend changes to GCP and FCP tasking as required by USTRANSCOM and the coordinating authority
- Develop assessment methodologies and metrics to support assessment of the GCPs and FCPs, IMOs and Effects
- Coordinate with USTRANSCOM, it's components and the JDDE to collect and evaluate data as part of the annual global and functional campaign plan assessments for each GCP and FCP
- Conduct GCP and FCP annual assessments for priority GCPs and FCPs as directed by higher authority
- Collect and prepare written feedback for the status of all GCP and FCP IMOs and Effects aligned to USTRANSCOM as either the lead or coordinating activity

FTE's supporting this task shall have a Top Secret/Sensitive Compartmentalized Information (SCI) clearance. The contractor support for this task shall be onsite. However, the contractor

may process unclassified and classified data at company site if he/she already have a government approved facility/systems for handling/storing classified information in order to provide the support requested above.

1.4.3. Task Area 3: Capability Development

This consists of functional activities relating to integrating several enterprise management processes pertaining to producing new capabilities for Logistics, Strategic Mobility, Distribution, and the Defense Transportation System. The contractor shall deliver products/services as outlined in below tasks, to include related TMT taskings, information papers, meeting minutes, video teleconference (VTC) set-ups, and presentations. The contractor support for this task area shall be onsite.

1.4.3.1. Integrated Priority List (IPL) Development

The contractor shall actively participate in the development of USTRANSCOM's annual IPL requirements in conjunction with Command Annual Joint Assessment (AJA) representative, OSD, JS, CCMDs, Services, and defense logistics agencies to identify deployment and distribution capability issues, shortfalls, and gaps supporting JDDE capability analysis, strategy development, investment decision making and capability development. The contractor shall provide the following support:

- Develop timeline and briefing to support annual IPL process.
    - Update templates as necessary based on TRANSCOM Commander's staff updates
    - Draft and submit initial timeline NLT 25 business days prior to the scheduled IPL kick-off meeting.
    - Submit final timeline and briefing NTL 3 business days prior to the scheduled kick-off meeting.
- Coordinate with USTRANSCOM Directorates, Components, and Subordinate Commands to develop IPL items that address JDDE, and USTRANSCOM Unified Command Plan (UCP) mission shortfalls and gaps related to ongoing efforts based on situational awareness gained during the performance of the task and working knowledge of the Joint Capabilities Integration and Development System (JCIDS).
- Support CP-GDD 9033 working group activities as they relate to IPL and CGA. The contractor shall have a working knowledge of the Planning, Programming, Budgeting and Execution (PPBE) and OSD and Joint Staff organizations/processes relating to the DOD Program Budget Review (PBR). The contractor shall have an understanding of how the IPL process impacts the Command's PBR Issue Nomination development process to provide analysis, administrative, and technical support.
- Maintain and utilize the IPL development tool (built in Microsoft Excel and/or Access) to capture Command IPLs and support proposed IPL item prioritization.
    - Update the IPL tool with the most current information throughout the IPL development process (Apr – Aug)
        - Initial update is due within 10 business days of IPL data receipt. Final update is due within 2 business days after IPL stakeholder prioritization meeting
        - Draft IPL point papers (one for each IPL item) from the IPL tool data within 2 business days after initial IPL tool update and final tool update

- Submit the final Command-approved IPL in the IPL tool, and properly integrate IPL data into the AJA as necessary to meet the Joint Staff deadline

FTE's supporting this task shall have Top Secret clearance/Sensitive Compartmentalized Information (SCI) clearance.". The contractor(s) supporting this task shall be onsite.

1.4.3.1.2. Capability Gap Assessment (CGA). Once the IPL is submitted into the Knowledge Management and Decision Support (KM/DS) system the contractor shall provide analysis, and administrative and technical support during the Capability Gap Assessment (CGA) Process. The contractor shall incorporate IPL changes resulting from the CGA process into the IPL tool. Post CGA IPL tool and IPL point paper final updates shall be completed NLT 10 business days following CGA Joint Capability Board (JCB) meeting. The contractor shall organize VTCs, draft and provide read-ahead materials for meetings, information papers, meeting minutes, and briefing presentations within 2 business days of task receipt.

FTE's supporting this task shall have Top Secret clearance/Sensitive Compartmentalized Information (SCI) clearance.". The contractor(s) supporting this task shall be onsite.

1.4.3.2. Joint Capabilities Integration and Development System (JCIDS) Gatekeeper
The contractor(s) shall have (or obtain within 60 days) a Level B JCIDS Certification IAW the JCIDS Manual. Working knowledge of the PPBE and familiarity with the CJCSI 5123 provides additional understanding for supporting the JCIDS related tasks. The contractor shall perform USTRANSCOM Gatekeeper tasks outlined in USTRANSCOM Instruction 3900.04. JCIDS Gatekeeper tasks are divided into three areas: meeting preparation and participation, document development, document coordination.

FTE's supporting this task shall have Top Secret clearance/Sensitive Compartmentalized Information (SCI) clearance.". The contractor(s) supporting this task shall be onsite.

1.4.3.2.1. JCIDS meeting support engagement
The contractor shall attend working groups, conferences, and meetings. Meetings include, but are not limited to, Functional Capabilities Board Working Group (FCB WG), FCBs, JCBs, and the Joint Requirements Oversight Council (JROC). The contractor shall coordinate activities supporting FCB WGs, FCBs, JCBs, and JROC. Support includes participating in and organizing VTCs. In coordination with appropriate Government Subject Matter Experts (SMEs) the contractor shall support research and review of topics in order to inform command decisions. Contractor shall review and research the topics submitted to the JCB and JROC and prepare correspondence with recommendations for USTRANSCOM senior leadership participation based on USTRANSCOM's equities. If USTRANSCOM has sufficient equity in a particular topic, the contractor shall coordinate pre-briefs for USTRANSCOM senior leadership, coordinate appropriate SME support, coordinate senior leader meeting participation, and interface with Joint Staff. The contractor(s) supporting this task shall be onsite.

FTE's supporting this task shall have Top Secret clearance/Sensitive Compartmentalized Information (SCI) clearance.". The contractor(s) supporting this task shall be onsite.

1.4.3.2.2. JCIDS document development.
The contractor shall provide JCIDS expertise supporting USTRANSCOM capability sponsors' development of formal products including, but not limited to, Initial Capabilities Documents (ICDs), Capability Development Documents (CDDs), Capability Production Documents (CPDs), and Doctrine, Organization, Training, Material, Leadership and Education, Personnel, Facilities and Personnel (DOTMLPF-P) Change Requests due within 2 business days after task receipt and finalize JCIDS review/coordination/guidance documentation NLT 2 days after receipt of Government comments. The contractor shall research, leverage, and synchronize related JCIDS actions to reduce redundancy and improve unity of effort. The contractor(s) supporting this task shall be onsite.

FTE's supporting this task shall have Top Secret clearance/Sensitive Compartmentalized Information (SCI) clearance.". The contractor(s) supporting this task shall be onsite.

1.4.3.2.3 JCIDS document coordination.
The contractor shall monitor and review daily JCIDS documents from the Knowledge Management and Decision Support (KM/DS) system for USTRANSCOM interest/equity and coordinate with appropriate SMEs to adjudicate documents. The contractor shall coordinate SME comments and input them into the KMDS system in appropriate format NLT 2 business days after receipt of Government comments. The contractor shall organize VTCs and read-ahead materials for meetings and provide information papers, meeting minutes, and briefing presentations within 2 days of task receipt. The contractor(s) supporting this task shall be onsite.

FTE's supporting this task shall have Top Secret clearance/Sensitive Compartmentalized Information (SCI) clearance.". The contractor(s) supporting this task shall be onsite.

2.0. SERVICE DELIVERY SUMMARY

2.1. Deliverables/Delivery Schedule
All references to days are defined as calendar or business days as specified.

PWS Task #	Deliverable	Schedule Draft	Final
1.4.1.1	Monthly Status Report (MSR)	Monthly	NLT 5 business days following month; final due last day of contract
1.4.1.2.	In-Process Review (IPR)	Slides due 5 business days prior to IPR	Quarterly

PWS Task #	Deliverable	Schedule Draft	Final
1.4.1.3.	Trip Report	As required	NLT 5 business days after travel completion
1.4.1.4	Employment Status Report	Annually or when personnel update	NLT 25 business days after contract award; changes due NLT 5 business days after any change in personnel
1.4.2.1 through 1.4.2.4.1	TMT support	Draft due date(s) as designated within TMT	Final due date as designated within TMT
1.4.2.1 through 1.4.2.4.1	Record and maintain meeting minutes	As required	NLT 3 business days after meeting
1.4.2.1 through 1.4.2.4.1	Prepare AARs for each staff visit, seminar, conference, IPR, etc.	As required	NLT 5 business days following event
1.4.2.1 through 1.4.2.4.1	Prepare documents, graphics, white papers, supporting papers and other materials in support of TMT tasking, point papers and/or presentations	As required	NLT 5 business days after receipt of government comments
1.4.2.1	Assist in design, layout and editing of the campaign plans, Campaign Plan Assessment (CPA), Global and Functional Campaign Plan Assessments, Command Strategy Forum (CSF) briefing materials and minutes, Joint Staff Action Packages (JSAPs), white papers, point papers and other campaign plan documents	Annually	NLT 5 business days after receipt of Government comments
1.4.2.1	Assess documents for gaps and inconsistencies and provide recommendations	As required	NLT 5 business days after government request

PWS Task #	Deliverable	Schedule Draft	Final
1.4.2.1	Preparation of presentation materials related to the logic and content of campaign clan publications to USTRANSCOM personnel, JDDE partners, and other personnel	As required	NLT 5 business days after government request
1.4.2.2	Manage NIPR and SIPR collaboration web sites, such as IntelShare and C2IE, in support of campaign planning and related tasks	As required	NLT 30 business days after contract award; changes due NLT 5 business days after receipt of government comments
1.4.2.2	Collect, collate, and distribute data as appropriate to aid campaign planning and assessment efforts	As required	NLT 30 business days after contract award; changes due NLT 5 business days after receipt of government comments
1.4.2.2	Develop and maintain a plan for the creation and storage of data on network drives separate from Intelshare websites	Annually	NLT 30 business days after contract award; changes due NLT 5 business days after receipt of government comments
1.4.2.2	Develop a storage structure to include file naming conventions and folder storage structure using government provided share drive resources	Annually	NLT 30 business days after contract award; changes due NLT 5 business days after receipt of government comments

PWS Task #	Deliverable	Schedule Draft	Final
1.4.2.2	Develop and maintain a standard campaign plans minutes format and archival process	Annually	NLT 30 business days after contract award for initial development; NLT 5 business days after receipt of government comments or change request
1.4.2.2	Distribute collected and collated data in support of campaign plans and the assessment process	As required	NLT 5 business days after receipt of government comments
1.4.2.2	Archive products, minutes, and briefs to include meeting minutes from the monthly Planners' forum, monthly CSFs, Campaign Planning Joint Planning Groups (JPG), and other products as directed by the government	Annually	NLT 5 business days after the start of a new quarter
1.4.2.2	Maintain NIPR and SIPR contact rosters for the JDDE community of interest (COI), and other contact lists as defined by the government	Quarterly	NLT 5 business days after the start of a new quarter
1.4.2.3	Facilitate sessions with USTRANSCOM, Defense Agencies, Services, CCMDs, OSD and the Joint Staff including, as required, senior officers or action officers, and other JDDE stakeholders as needed to support the JDDC's guidance, provide read ahead materials as appropriate	As required	NLT 2 business days prior to facilitated session
1.4.2.3	Author, edit, and recommend change to strategic guidance, joint publications, and other guidance in accordance with the specified review cycle	As required	NLT 5 business days after receipt of Government comments

PWS Task #	Deliverable	Schedule Draft	Final
1.4.2.3	Author, edit, and recommend change to campaign base plans, annexes, and associated attachments as required in accordance with Strategic Guidance, Joint Publications, Joint Operation Planning, Chairman of the Joint Chiefs of Staff Instructions and Manuals, and CDRUSTRANSCOM guidance	As required	NLT 5 business days after receipt of Government comments
1.4.2.3	Review supporting and complimentary plans (e.g., NSS, UCP, NDS, GEF, NMS, JSCP, GCP, CCMD Campaign Plans, FCP, TDP and TPPs), directives, and doctrine in accordance with government criteria to ensure alignment with all DOD Plans	As required	NLT 5 business days after receipt of Government comments
1.4.2.3	Support TCJ5-GP in collaborative JDDC process activities (e.g., conferences, seminars, VTCs, DCOs, staff coordination, etc.)	As required	NLT 5 business days after receipt of Government comments
1.4.2.3	Conduct coordination activities by providing support to Supported Command planners, their component planners, and USTRANSCOM component planners, Joint Staff, DLA and other supporting agency participants in preparation for and during seminars	As required	NLT 3 business days prior to activities
1.4.2.3	Provide multimodal, distribution, transportation and logistics planning, subject matter expertise for USTRANSCOM and TCJ5/J4 at meetings, seminars and conferences to discuss the USTRANSCOM JDDE responsibilities, the campaign planning process and other issues affecting deployment and distribution coordination across the DOD	As required	NLT 5 business days after receipt of Government comments

PWS Task #	Deliverable	Schedule Draft	Final
1.4.2.3	Attend events as representation for TCJ5/J4, to include but not limited to National Defense Transportation Association (NDTA), Commander's Call, Directorate Calls, war-games, and exercises, as directed by the government,	As required	NLT 5 business days after receipt of Government comments
1.4.2.3	Prepare LOE reporting using the format provided by the government in support of the assessment process	As required	NLT 5 business days after receipt of Government comments
1.4.2.3	Assist Line of Effort (LOE) leads in determining the alignment of gaps and seams in the JDDE to intermediate objectives found in FCP-GDD and USTRANSCOM CCP	Quarterly	NLT 5 business days prior to the quarterly CSF
1.4.2.3	Prepare and consolidate briefings to the CSF and other USTRANSCOM governance forums	Quarterly	NLT 3 business days prior to meeting
1.4.2.3	Submit detailed CSF meeting minutes no later than 5 business days after the completion of a CSF. CSF meeting minutes shall document the content of the CSF, to include tasks assigned, OPRs for each task, and results of CSF voting	As required	NLT 5 business days after the CSF
1.4.2.3	Support the creation of any briefs and TMTs required of the Campaign Planning team as a result of proceedings at the CSF	Quarterly	NLT 5 business days after the CSF
1.4.2.3	Collect and adjudicate FCP-GDD campaign plans comments and requests for revision from USTRANSCOM and other JDDE partners	As required	NLT 5 business days after receipt of comments
1.4.2.3	Assist the government in preparation of and delivery of FCP-GDD campaign plan training, integrated planning teams, and IPR	As required	NLT 5 business days after request for support

PWS Task #	Deliverable	Schedule Draft	Final
1.4.2.4	Collect information from internal and external sources to support campaign plan Assessments	Quarterly	NLT 5 business days after receipt of Government comments
1.4.2.4	Aggregate and analyze collected information in support of monthly campaign plan assessments	Quarterly	NLT 5 business days after receipt of Government comments
1.4.2.4	Conduct monthly CCP LOE assessments	Monthly	NLT 5 business days after receipt of Government comments
1.4.2.4	Prepare CSF assessment briefings in support of LOE leads and the CSF	Monthly	NLT 5 business days after receipt of Government comments
1.4.2.4	Interpret assessment results and provide recommendations to the government	As required	NLT 15 business days after request of the government
1.4.2.4	Solicit, collect, aggregate, and prepare USTRANSCOMs response to the AJA	Annually	NLT 15 business days after request of the government
1.4.2.4	Conduct GDA assessment in accordance with government procedures	Annually	NLT 15 business days after request of the government
1.4.2.4	Prepare campaign plan assessments, AJA, and GDA products, processes, frameworks, and effectiveness measures	As required	NLT 5 business days after request by the government
1.4.2.4	Provide briefing materials for campaign plan assessment, AJA, and GDA findings and recommendations	As required	NLT 3 business days prior to brief

PWS Task #	Deliverable	Schedule Draft	Final
1.4.2.4	Assist the government in developing campaign plan assessments, AJA, and GDA products, processes, frameworks, and effectiveness measures	As required	NLT 5 business days after interactions
1.4.2.4.1	Coordinate with the Joint Staff, CCMDs, and designated coordinating authorities on the assessment of global and functional campaign plans	As required	NLT 5 business days after interactions
1.4.2.4.1	Provide comments on interactions with Joint Staff, CCMDs, and designated coordinating authorities on the assessment of GCPs.	As required	NLT 5 business days after interactions
1.4.2.4.1	Identify, evaluate, and recommend changes to USTRANSCOM aligned GCP and FCP IMOs and Effects.	As required	NLT 15 business days after receipt of government comments
1.4.2.4.1	Develop assessment methodologies and metrics in support of GCP and FCP assessments	Annually	NLT 20 business days after request by the government
1.4.2.4.1	Coordinate with USTRANSCOM, it's components and the JDDE to collect and evaluate data as part of the annual global and functional campaign plan assessments for each GCP and FCP	Annually	NLT 5 business days after receipt of Government comments
1.4.2.4.1	Conduct GCP and FCP annual assessments for priority GCPs and FCPs	Annually	NLT 5 business days after receipt of Government comments
1.4.2.4.1	Collect and prepare written feedback on the status of all GCP and FCP IMOs and Effects task assigned to USTRANSCOM	Annually	NLT 15 business days after request by the government
1.4.3. through 1.4.3.2	Provide support and inputs for information Papers, meeting	Within 2 business days of Government tasking	2 business days after receipt of

PWS Task #	Deliverable	Schedule Draft	Final
	minutes, and briefing presentations		Government comments
1.4.3. through 1.4.3.2	Provide direct support for assigned task within Task Management Tool (TMT)	Draft due date(s) as designated within TMT	Final due date as designated within TMT
1.4.3.1	IPL timeline and initial kick-off briefing	NLT 25 business days prior to scheduled kick-off meeting	NLT 3 business days prior to scheduled IPL kick-off meeting
1.4.3.1.	Initial update of IPL candidate data in the IPL tool	10 business days after receipt of IPL data from sponsor	2 business days after IPL stakeholder prioritization meeting
1.4.3.1	Final update of IPL data into the IPL Tool and AJA	2 business days after final IPL approval	Integrate IPL data into KM/DS NLT the suspense provided by the Joint Staff.
1.4.3.1.	IPL Point Papers	2 business days after initial IPL tool update	2 business days after final IPL tool update
1.4.3.1.	Post CGA IPL tool and Point Paper updates	As required	10 business days following CGA JCB meeting
1.4.3.2.	Review KM/DS for USTRANSCOM interest/equity items, advise Government lead	Daily	Daily
1.4.3.2.	Joint Capabilities Integration and Development System (JCIDS) review /coordination /guidance documentation	2 business days after tasking receipt	NLT 2 business days after receipt of Government comments
3.9.2.	Transition Plan		60 calendar days prior to the contract end date
3.9.2.	Update on open tasks		5 business days prior to the contract end date
5.2	Provide timely cyber-incident reporting.		No more than one late cyber-incident report or unreported cyber-

PWS Task #	Deliverable	Schedule Draft	Final
			incident in a twelve (12) month period.

2.2. Performance Objectives

The Service Delivery Summary (SDS) represents important contract objectives that, when met, will ensure contract performance is satisfactory. Although not all PWS requirements are listed in the SDS, the contractor is fully expected to comply with all requirements in the PWS delivered in accordance with the following performance objectives.

PWS Task #	Performance Objective	Performance Threshold
1.3.1.1.	Monthly Status Report	On time submission. No more than two customer complaints per report.
1.3.	Stated deliverables are timely and accurate	Delivered in accordance with the PWS schedule with 95% accuracy.

3.0 GENERAL INFORMATION

3.1. Government Furnished Equipment/Information (GFE/GFI)

GFP will be provided for this task order as indicated in the GFP attachment included with the solicitation, distributed at award, and incorporated via the GFP Module in PIEE. GFP shall be managed IAW the terms of FAR 52.245-1, corresponding GFP DFARS clauses, and any additional instructions incorporated at award.

There is ONE GFP Attachment for the task order that identifies any GFP the contractor is authorized to have in their possession. Any changes to the GFP Attachment over the life of the contract require both a contract modification and a GFP Attachment update to create a consolidated, conformed list of authorized GFP.

The GFP Attachment is a single consolidated document that identifies contract information, serially managed GFP items, non-serially managed GFP items, and items for which the contractor is given requisitioning authority which are paid for by USTRANSCOM.

- Serially managed items are provided to the contractor by USTRANSCOM and require all events identified in DFARS 252.211-7007 to be reported by the contractor.
- Non-serially managed items are provided to the contractor by USTRANSCOM and require only the event of GFP receipt to be reported.
- Items that are authorized to be requisitioned by the contractor and paid for by USTRANSCOM are listed on the Requisitioned Items section. Note that items for which the contractor has authorization to requisition, which are paid for by the contractor, are considered Contractor Furnished Material and are therefore NOT identified on the GFP Attachment.

Both the Government and the contractor shall retain copies of any GFP listings for traceability and accountability. GFP provided to the contractor and used at the contractor facility shall be managed and controlled by the contractor.

The contractor shall be responsible for providing workstations, peripherals, and any Commercial-off-the-Shelf (COTS) as required for employees working off-site which do not need access to Government-owned networks and resources. The use of privately owned computers (i.e., computers not owned and provided by USTRANSCOM) to process classified information is prohibited. Neither personally owned hardware nor software will be used in the official conduct of Government business, nor will it be installed on USTRANSCOM information assets for personal use or gain. Additionally, use of entertainment and games software is prohibited.

The Property Transfer capability in the GFP Module enables contractors to report receipt of all GFP and to report receipt, shipment, consumption, disposal, or transfer to another contract of serially managed GFP in accordance with DFARS 252.211-7007. The capability also enables USTRANSCOM to create shipment documents of GFP moving to a contractor and to acknowledge receipt of returned GFP.

The GFP Position Report accessible in EDA provides a near real-time view of GFP in the contractor's custody. The Property Transfer capability reuses data from the GFP Attachment to create shipment or receipt documents. Because the GFP Module keeps track of GFP receipted in the Module by the contractor, GFP items returning to USTRANSCOM can be selected from previously receipted items and the items will be removed from the contractor's accountable items list in the GFP Module.

The process should begin when USTRANSCOM creates a shipment document in the Property Transfer capability area of the GFP Module, either by selecting items from the GFP Attachment or adding them manually. Items identified as shipped to a contractor that are not on the GFP Attachment will trigger a discrepancy email to the GFP Attachment approver to alert them that the physical world is different from what is authorized and an update to the GFP Attachment may be needed. The contractor will receive an email alerting them of inbound GFP.

When the items physically arrive at the contractor's facility, the contractor will use the shipment document in the GFP Module to acknowledge receipt. The shipper will receive email notification that the items have been received by the contractor.

Even if the USTRANSCOM shipper did not create a shipment document in the GFP Module, the contractor must still report receipt of the GFP in the GFP Module to comply with DFARS 252.211-7007. The contractor is required to report receipt of all GFP regardless of if there is a shipment document or a GFP Attachment.

To return GFP to USTRANSCOM (or send it to another contractor), the custodial contractor will create a shipment document in the GFP Module selecting from previously receipted items. The items will be removed from the contractor's accountable item list and the GFP Position Report will no longer include the shipped items. When the items are physically at the recipient's site, the recipient will acknowledge receipt against the shipment document.

Property shipment or receipt data may be manually entered via the web, submitted by X.12 or flat file electronic format, or uploaded via Excel. The Excel template can be downloaded from the "Information" area to the right.

Contractors in possession of GFP shall provide the COR an annual report of all GFP in their possession, to include the item description, make, model, serial number, IUID, and last inventory date. The report should be minimally provided on an annual basis and 30 days prior to the expiration of any performance period (base and options).

Software provided by the Government and used at contractor facilities will be treated as GFE. The contractor shall release all GFE to the Government upon termination of the specific task or subtask, whichever date is earlier.

Employees requiring access to Government-owned networks and resources will be provided workstations/laptops, peripherals, and any COTS by the Government, both off-site and on-site. Access to the Government resources from off-site locations will require use of Government's CAC-enabled Virtual Private Network (VPN) technologies on the all Government-issued workstations or the use of Government's CAC-enabled Virtual Desktop Infrastructure (VDI) technologies.

3.2. Place of Performance

Due to the security nature of the tasks the primary place of performance for all services is Scott AFB, IL. The Government will provide workspace for up to eleven (11) contractor personnel to work on-site at the Government facility located at Scott Air Force Base, IL. Any unforeseen circumstances limiting on-site availability, i.e., natural disaster or widespread global situation, will be handled on a case by case basis with the government making the final determination on acceptable alternate work sites.

3.3. Hours of Operation and Recognized Holidays

The Contractor shall provide support during normal Government business hours between 0700-1600 hours central time, Monday through Friday, excluding Federal Government holidays. Contract support hours are subject to change due to increased requirements for operations outside the normal workday, and contractors may be required to provide support outside normal business hours based on operational requirements. The contractor shall ensure sufficient personnel are available at the Government site during these hours to allow for emerging requirements during the workday with the Government (i.e., the hours of individual employees may be staggered but the contractor shall have coverage for the entire 9-hour period). For contractor site performance, the contractor shall ensure sufficient personnel are available during the same hours as Government site personnel to allow for interaction with the Government during normal duty hours, 0700-1600 Central Time Zone. The following will be observed as Federal Government holidays: New Year's Day, Martin Luther King's Birthday, President's Day, Memorial Day, Juneteenth, Independence Day, Labor Day, Columbus Day, Veteran's Day, Thanksgiving Day, and Christmas Day. Note: Any of the above holidays falling on a Saturday shall be observed on the preceding Friday. Holidays falling on a Sunday shall be observed on the following Monday.

3.4. Period of Performance
Base Period is 01 October 2023 through 30 September 2024.
First Option Period is 01 October 2024 through 30 September 2025.
Second Option Period is 01 October 2025 through 30 September 2026.
Third Option Period is 01 October 2026 through 30 September 2027.
Fourth Option Period is 01 October 2027 through 30 September 2028.

3.5. Travel
Performance under this contract may require the contractor travel within the Continental United States. The Government will reimburse the contractor for travel expenses subject to FAR 31.205-46, Travel Costs, and Joint Travel Regulation. The Government will not pay profit on travel but will allow the contractor to charge General and Administrative overhead for travel approved under this paragraph. All contractor travel shall be coordinated with and validated by the primary or alternate COR prior to incurring travel expenses. The contractor shall identify personnel who will be traveling in sufficient time to obtain the lowest possible rates for airfare, rental car and lodging. For long distance travel, a minimum of five business days advance notice from the travel commencement date is required unless mission requirements dictate otherwise. The travel request shall be in writing and contain the dates, location, and estimated travel costs. Contractor invoices (along with associated receipts) shall support all travel reimbursement requests. Actual travel costs will be reported in a trip report to the COR by person, by trip within five business days of completion of travel. The Government will not reimburse local travel and related expenses to the contractor for daily travel to or from Scott AFB or the contractor's facility.

3.6. Quality Assurance
The contractor shall support Government agency reviews and audits of all services and support provided under this PWS. The contractor shall be prepared to support Quality Assurance reviews conducted by the Government. The Government reserves the right to authorize an independent verification and validation of the contractor’s procedures, methods, data, equipment, and other services provided at any time during the performance of this PWS.

3.7. Non-Disclosure Agreements (NDA)
In performance of this contract, the Contractor will have access to sensitive, non-public information. The contractor agrees (a) to use and protect such information from unauthorized disclosure IAW DTM 08-027 - Security of Unclassified DOD Information on Non- DOD Information Systems, 31 July 2009; (b) to use and disclose such information only for the purpose of performing this contract and to not use or disclose such information for any personal or commercial purpose; (c) to obtain permission of the Government before disclosing/discussing such information with a third party; (d) to return and/or electronically purge, upon Government request, any non-public, sensitive information no longer require for contractor performance; and (e) to advise the Government of any unauthorized release of such information. Upon request, the contractor shall have its employees assigned to this contract execute a non-disclosure agreement for delivery to the Government. The Government will require contractor personnel to sign a non-disclosure statement to protect non-public information of other contractors and/or the Government. The NDA is Appendix 2.

3.8. Planning, Programming, Budget, and Execution Data

The contractor may be required to access and protect DOD Planning, Programming, Budget, and Execution (PPBE) data in the performance of this contract. The required PPBE NDA is Appendix 3. For the purposes of this contract, PPBE means any information that sets forth defense programs or budgets of the Department of Defense, its components, or other government agencies. PPBE information includes, but is not limited to:

(a) Planning Documents and Data Sources that contain traditional PPBE information concerning budgeting and programs

(b) Programming Documents and Data Sources

(1) Joint Programming Guidance

(2) Fiscal Guidance (when separate from Strategic Planning or Joint Programming Guidance)

(3) Program/Budget displays generated through the Program Data Requirements process

(4) Program Objective Memorandum/Budget Estimate Submission Future Years Defense Plan (POM/BES FYDP) documents and associated Office of the Director, Program Analysis & Evaluation (OD, PA&E) data systems such as the Defense Programming Database Data Warehouse

(5) Program Review Proposals and associated documents, including:

(i) Issue Outlines

(ii) Program Change Proposals

(iii) Issue Papers/Briefings

(iv) Issue Summaries

(6) Proposed Military Department Program Reductions (or Program Offsets)

(7) Tentative Issue Decision Memoranda

(8) Program Decision Memoranda

(9) Cost Analysis Improvement Group Independent Cost Estimates

(c) Budgeting Documents and Data Sources

(1) Component budget submissions, including:

(i) Budget Change Proposals

(ii) Budget Estimate Submissions

(iii) Justification material in support of a component's submission

(2) PPBE decision documents, including:

(i) Program Budget Decisions

(ii) Management Initiative Decisions

(3) Reports or the results of queries from the Comptroller Information System or the Procurement, RDT&E and Construction Program systems

(4) Classified P-1, R-1, Procurement Programs, and RDT&E Programs documents

(5) DD 1414, "Base for Reprogramming Action"

(6) DD 1416, "Report of Programs"

Access to PPBE documents and data is restricted by DOD Directive 7045.14, "The Planning, Programming and Budgeting System (PPBS)", and Deputy Secretary of Defense Memorandum, "Control of Planning, Programming, Budgeting and Execution (PPBE) Documents and Information". Permission to access PPBE data must be granted by the OSD Cost Assessment and Program Evaluation (CAPE) Office.

Contractors shall not have access to PPBE documents and information unless all Contractor employees performing work under a contract for whom access privileges are requested have signed a nondisclosure agreement. The Contractor shall ensure that each Contractor employee and each subcontractor employee who is to have access to PPBE information in connection with this contract executes the PPBE NDA at Appendix 3 of this PWS. The Contractor shall provide each executed PPBE NDA to the COR. No person shall have access to PPBE information unless his or her executed PPBE NDA is provided to the COR. The NDAs must remain on file for the duration of this contract.

The Contractor shall not disclose PPBE information obtained in connection with this contract to any person or entity (including, but not limited to, any subcontractor or employee of the Contractor) without written authorization from the Contracting Officer. The Contractor shall promptly notify the Contracting Officer of (a) any unauthorized disclosure of PPBE, or (b) any attempt by any person or entity (including, but not limited to, any subcontractor or employee of the Contractor) to gain unauthorized access to PPBE. Such notification shall identify each person or entity making or receiving the disclosure or each person or entity making the attempt.

3.9. End of Contract Transition.

3.9.1. Ending Overlap Period

The contractor shall provide operational familiarization, i.e., will work side-by-side with a successor contractor on the local processes and procedures for performance of day-to-day duties, specifically deliverables. This effort is not functional training but is to familiarize the incoming contractor with the USTRANSCOM work environment as it relates to the requirements of the PWS. Overlap period will be limited to 20 business days.

3.9.2. Transition Planning

Sixty (60) calendar days prior to end of the contract period, the contractor shall organize all work-related documents and files, store them on the designated shared drives, and provide a file plan outlining the file structure. Status for each project shall be documented, to include recent, current, and pending actions.

The contractor shall provide soft copies of all procedures and training materials developed as part of the contract. In addition, the contractor shall provide a complete list of all badges, vehicle passes, and Government software access permissions by individuals currently working on the contract. The contractor must ensure no logistics or contract data is corrupted, changed, or altered in a manner that would cause damage to the Government. The contractor shall meet performance requirements and cooperate with the successor contractor in the transition period.

The contractor shall provide the assistance and support required to ensure the orderly transition of all support and provide transitional planning necessary to enable the follow-on contractor to commence uninterrupted operations at the end of the contract period. The contractor shall ensure follow-on contractor personnel are permitted access to observe all operations, including workflow, priorities, scheduling, equipment handling/processing, parts storage, safety, and security.

Familiarization visits shall not interfere with the activities of the incumbent contractor or Government personnel.

3.9.3. Continuity of Service

The contractor shall ensure the continuity of service while implementing its transition plan for all affected activities to preclude any adverse impact on the mission. To ensure continuity is maintained through transition, the contractor and the incoming contractors shall have an overlap period not to exceed 20 business days to ensure incoming contractors are familiar with specific tasks to be performed IAW section 1.4. of this PWS.

3.9.4. Transfer of Materials

The contractor shall transfer to the Government all intellectual property belonging to the Government which was generated or provided by the Government for the performance of this contract. The contractor shall organize all work-related documents and files, store them on CDs and/or DVDs, and provide a file plan outlining the file structure. In addition, the contractor shall provide a complete list of all badges, vehicle passes, and Government software access permissions by individual currently working on the contract. The contractor must ensure no logistics or contract data is corrupted, changed, or altered in a manner that would cause damage to the Government.

3.9.5. Cooperative Work Environment

The contractor shall maintain a cooperative work environment with other Government contractors and personnel (so as not to cause interference, disagreement, or delays to work to be performed) while not compromising health, safety or security. The contractor shall be responsible for adapting schedules and performance to accommodate additional support work. Conflicts or cause for delays shall be brought to the attention of the COR.

3.9.6. Other Direct Costs (ODC)

The Government will reimburse allowable ODCs incurred in the performance of this PWS. ODCs may include, but are not limited to, printing of materials for conference or seminar attendance i.e., NDTA and other local conferences, war-games, local exercises, commander's calls. The contractor shall submit ODC requests in writing to the COR for approval at least five business days in advance of incurring any expenses. The request shall contain estimated costs supported by a minimum of three competitive quotes. Contractor invoices (along with associated receipts) shall support all ODC reimbursement requests. In no event shall the contractor be authorized to purchase ODCs that exceed the ODC amount funded in the contract. General and Administrative overhead charges will not be accepted or paid for approved ODC purchases.

3.9.7. Health and Safety on Government Installations

In performing work under this contract on a Government installation, the contractor shall:

(a) Take all reasonable steps and precautions to prevent accidents and preserve the health and safety of contractor and Government personnel performing or in any way coming in contact with the performance of this contract; and
(b) Take such additional immediate precautions as the contracting officer may reasonably require for health and safety purposes.

3.9.7.1. Changes to Health and Safety Standards
The contracting officer may, by written order, direct health/safety standards as may be required in the performance of this contract and any adjustments resulting from such direction will be in accordance with the Changes clause of this contract.

3.8.7.2. Violations to Health and Safety Rules and Requirements
Any violation of these health and safety rules and requirements, unless promptly corrected as directed by the contracting officer, shall be grounds for termination of this contract in accordance with the Default clause of this contract.

3.8.8 Identification of Potential Organizational Conflict of Interest (OCI)
All personnel (military, Government civilian, and support contractor) within the TCJX will have access and work with acquisition/proprietary information governed by Federal Acquisition Regulation (FAR). Organizational conflict of interests shall be avoided, neutralized or mitigated IAW FAR 9.505.

3.8.9. Non-Personal Services.
This requirement is for a "non-personal services contract" as defined in FAR 37.101. PERSONAL SERVICES CONTRACTS ARE EXPRESSLY PROHIBITED BY 5 U.S.C. 3109 AND FAR SUBPART 37.1

3.8.9.1. Contractor Employees
It is, therefore, understood and agreed the contractor and/or the contractor's Employees: (1) shall perform the services specified herein as independent contractors, not as employees of the Government; (2) shall be responsible for their own management and administration of the work required and bear sole responsibility for complying with any and all technical, schedule, or financial requirements or constraints attendant to the performance of this contract; (3) shall be free from supervision or control by any Government employee with respect to the manner or method or performance of the services specified; but (4) shall, pursuant to the Government's right and obligation to inspect, accept or reject the work, comply with such general direction of the CO, or the duly authorized representative of the CO, as is necessary to ensure accomplishment of the contract objectives.

3.8.9.2. Government Employer-Employee Management clarification
This requirement shall not be administered in a manner that makes it a personal services contract. A personal services contract is a contract that is administered in a manner that makes contractor personnel appear, in effect, to be Government employees. The relationship between the Government managers and contractor employees resembles an employer-employee relationship. In personal services situations there is relatively continuous supervision and control of contractor employees by Government employees.

3.8.9.3. Decision Making
The contractor is not authorized to make decisions on behalf of the Government. The contractor shall make recommendations to Government personnel for the Government's decision- making purposes.

3.8.9.4. Contractor Employee Management
Contractor employees performing services under this contract shall be controlled, directed, and supervised at all times by management personnel of the contractor. The contractor's management shall ensure that employees properly comply with the performance standards outlined in this PWS and as required by the CO or COR. Contractor employees shall be capable of performing independently and without the assistance of Government personnel. Actions of contractor employees shall not be interpreted or implemented in any manner which results in a contractor employee creating, modifying, or violating Federal policy, obligating the appropriated funds of the U.S. Government, overseeing the work of Federal employees, providing direct personal services to any Federal employee, or otherwise violating the prohibitions set forth in FAR Parts 7.5 and 37.1. If the contractor feels that any actions constitute or are perceived to constitute personal services, it shall be the contractor's responsibility to notify the COR immediately.

3.8.9.5. Inherent Government Work Clarification
No contractor personnel will perform any work on this contract that can be defined as inherently governmental according to FAR Subpart 7.503(c). Contractor personnel will be performing tasks under FAR Subpart 7.503(d); however, contract personnel will be in a supporting role to the Government task lead and will not be in a decision-making role. The Government shall be the sole authority for decisions.

4.0. CYBERSECURITY

4.1. Operationally Critical Support

The services designated under this contract are "operationally critical support" as defined in DFARS 252.204-7012.

4.2. Cybersecurity Incident Reporting

4.2.1. In addition to the DFARS 252.204-7012 reporting requirements for unclassified systems and DoD Manual (DoDM) 5220.22, National Industrial Security Program Operating Manual (NISPOM) for classified systems, reportable cyber-incidents include, but are not limited to, the following:

4.2.1.1. Cyber-incidents as defined in Table 1.

4.2.1.2. Notifications by a federal, state, or local law enforcement agency or cyber-center (i.e., National Cyber Investigative Joint Task Force (NCIJTF), National Cybersecurity & Communications Integration Center (NCCIC)) of being a victim of a successful or unsuccessful cyber-event, anomaly, incident, insider threat, breach, intrusion, or exfiltration.

Table 1.

Incident Category	Description
Root Level Intrusion	Unauthorized privileged access to an IS. Privileged access, often referred to as administrative or root access, provides unrestricted access to the IS. This category includes unauthorized access to information or unauthorized access to account credentials that could be used to perform administrative functions (e.g., domain administrator). If the IS is compromised with malicious code that provides remote interactive control, it will be reported in this category.
User Level Intrusion	Unauthorized non-privileged access to an IS. Non-privileged access, often referred to as user level access, provides restricted access to the IS based on the privileges granted to the user. This includes unauthorized access to information or unauthorized access to account credentials that could be used to perform user functions such as accessing Web applications, Web portals, or other similar information resources. If the IS is compromised with malicious code that provides remote interactive control, it will be reported in this category.
Denial of Service	Denial of Service (Incident)—Activity that denies, degrades, or disrupts normal functionality of an IS or DoD information network.
Malicious Logic	Installation of software designed and/or deployed by adversaries with malicious intentions for the purpose of gaining access to resources or information without the consent or knowledge of the user. This only includes malicious code that does not provide remote interactive control of the compromised IS. Malicious code that has allowed interactive access should be categorized as Root or User Level Intrusion incidents. Interactive active access may include automated tools that establish an open channel of communications to and/or from an IS.
Ransomware	Malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. Ransomware actors often target and threaten to sell or leak exfiltrated data or authentication information if the ransom is not paid. Ransomware is a reportable incident that may be associated with multiple incident categories depending on the attack vector and execution.

4.2.2. If the cyber-incident affects a classified system, vulnerabilities associated with the incident will be classified per the current version of USTRANSCOM Instruction 31-02, Security Classification Guide.

4.3. Cybersecurity Incident Reporting Timelines

In addition to providing the notification required by DFARS 252.204-7012, the contractor is required to notify USTRANSCOM as soon as practical, but no later than 72 hours after discovering a reportable cyber-incident. The reporting timeline begins when the incident is

discovered or reported to the company, its employees, contractors, or cybersecurity firm responsible for providing cybersecurity and response for the company. The contractor shall contact the USTRANSCOM Cyber Operations Center (CyOC) via phone at 618-220-4222. If the contractor does not immediately reach the CyOC via phone, the contractor shall send an email notification to transcom.scott.tcj6.mbx.cyoc@mail.mil.

4.4. Mandatory Reporting Data

4.4.1. The contractor shall work with the USTRANSCOM CyOC through resolution of the incident. Within 72 hours of becoming aware of a reportable cyber-incident, the contractor shall provide an initial notification of the incident, even if some details are not yet available, which includes, but is not limited to, the following information:

(a) Company Name
(b) Who will be the POC with contact information
(c) Contracting Officer POC (name, telephone, email)
(d) Overall Assessment –Description of incident, data at risk, mitigations applied
(e) Indicators of compromise
(f) Vector of attack (if known)
(g) Estimated time of attack (if known)

4.4.2. The contractor shall provide a follow-on cyber-incident report to the USTRANSCOM CyOC within 5 days of becoming aware of a reportable cyber-incident, which includes, but is not limited to, the following information:

(a) Contractor unique Commercial and Government Entity (CAGE) code
(b) Contract numbers affected
(c) Facility CAGE code where the incident occurred if different than the prime Contractor location
(d) POC if different than the POC recorded in the System for Award Management (name, address, position, telephone, email)
(e) Contracting Officer POC (name, telephone, email)
(f) Contract clearance level
(g) DoD programs, platforms, systems, or information involved
(h) Location(s) of compromise
(i) Date incident discovered
(j) Type of compromise (e.g., unauthorized access, inadvertent release, other)
(k) Description of technical information compromised
(l) Any additional information relevant to the information compromise

4.5. Incident Reporting Coordination

4.5.1. In the event of a cyber-incident, USTRANSCOM may conduct an on-site review of network or information systems where DoD information is resident on or transiting to assist the contractor in evaluating the extent of the incident and to share information in an effort to

minimize the impact to both parties. Date and time of on-site visits will be mutually agreed upon by USTRANSCOM and the contractor in advance.

4.5.2. The contractor agrees to allow follow-on actions by the Government (e.g., USTRANSCOM, Federal Bureau of Investigation, Department of Homeland Security, DC3, etc.) to further characterize and evaluate the suspect activity. The contractor acknowledges that damage assessments might be necessary to ascertain an incident methodology and identify systems compromised as a result of the incident. Once an incident is identified, the contractor agrees to take all reasonable and appropriate steps to preserve any and all evidence, information, data, logs, electronic files and similar type information (reference NIST Special Publication 800-61, Computer Security Incident Handling Guide, (current version)) related to the incident for subsequent forensic analysis so that an accurate and complete damage assessment can be accomplished by the Government.

4.5.3. The contractor is not required to maintain an organic forensic capability, but must ensure data is preserved (e.g., remove an affected system, while still powered on, from the network) and all actions documented until forensic analysis can be performed by the Government or, if the Government is unable to conduct the forensic analysis, a mutually agreed upon third party (e.g., Federally Funded Research and Development Center (FFRDC), commercial security contractor, etc.). Any follow-on actions shall be coordinated with the contractor via the Contracting Officer.

4.5.4. The contractor agrees to indemnify and hold the government harmless for following any recommendations to remedy or mitigate the cyber-incident following the actions under 1.5.1. and 1.5.2.

4.6. Confidentiality and Non-Attribution Statement

The Government may use and disclose reported information as authorized by law and will only provide attribution information on a need-to-know basis to authorized persons for cybersecurity and related purposes (e.g., in support of forensic analysis, incident response, compromise or damage assessments, law enforcement, counterintelligence, threat reporting, and trend analysis). The Government may share threat information with other USTRANSCOM industry partners without attributing or identifying the affected contractor.

5.0. SECURITY (PHYSICAL, PERSONNEL, INFORMATION, ANTITERRORISM/ FORCE PROTECTION AND INDUSTRIAL)

5.1. General Security Information

The majority of daily work associated with this PWS is at the unclassified level, but contractor personnel may be required to access SECRET information and/or classified areas, during performance of this task order.

5.2. Citizenship and Clearance Requirements

The contractor's, subcontractors, and/or partner's personnel performing services under this task order shall be citizens of the United States of America. Overall, all contractor personnel shall possess the appropriate personnel security investigation for the position(s) occupied. Contractor

personnel shall be required to have a background investigation that corresponds with the sensitivity level of the tasks to be performed. Note that neither dual citizens nor non-US citizens are eligible for Common Access Cards (CACs) unless they meet the parameters stated in DoDM 1000.13, volume 1.

5.3. Clearance Requirements and Position Sensitivity

Contractor personnel with IA administrative privileges and/or who will monitor DOD IT systems or software as designated by DOD Instruction 8500.1 and DOD Manual 5200.02 may be rated at the various levels listed below. The stipulation of the numbers and what IT/Automated Data Processing (ADP) levels the contractors will have been approved by the COR or the CO before the start of the task order. The contractor shall comply with all appropriate provisions of applicable security regulations while assigned to this task order for DOD and USTRANSCOM. The following guidance will be followed when determining background investigation and clearance levels for this task order depending on requirements:

POSITION LEVEL:
Information Technology (IT)-II
Automated Data Processing (ADP)-II
Or Non-Critical Sensitive Positions (SECRET):
IT/ADP-II and Non-Critical Sensitive Positions are those positions that: have access to Secret or Confidential information; Security police/provost marshal-type duties involving the enforcement of law and security duties involving the protection and safeguarding of DOD personnel and property; category II automated data processing positions; duties involving education and orientation of DOD personnel; duties involving the design, operation, or maintenance of intrusion detection systems deployed to safeguard DOD personnel and property; responsible for the direction, planning, design, operation, or maintenance of a computer system, and whose work is technically reviewed by a higher authority of the ADP-I category to ensure the integrity of the system; and any other position so designated by the head of the Component or designee.

BACKGROUND INVESTIGATION REQUIREMENTS:
(IT-II/ADP-II/Non-Critical Sensitive) Requirements for SECRET – (Tier 3):
Positions designated by the Government at the Non-Critical Sensitive/ADP-II/IT-II rating require a Tier 3 (or acceptable periodic reinvestigation) favorably adjudicated (a favorable adjudication grants eligibility at the SECRET level as prescribed by DODM 5200.02). The IT-II/ADP-II requirement mandates the contractor have a minimum Facilities Clearance Level at the SECRET (or higher) level due to investigation submissions as directed in DOD 5220.22-M Operating Manual, DODM 5200.01 and Defense Information Security System (DISS).

POSITION LEVEL:
Information Technology (IT)-III
Automated Data Processing (ADP)-III
Or Non-Sensitive Positions (Position of Trust Determination) (No Classified Access–Tier 1)
All other positions involved in computer activities and Common Access Card. No clearance is granted for classified access and only a Position of Trust (PoT) is awarded and posted in DISS.

BACKGROUND INVESTIGATION REQUIREMENTS:

(Non-Sensitive/IT-III/ADP-III) Requirements for Position of Trust Determinations (No Classified Access - Tier 1/NACI):
Positions designated by the Government as Non-Sensitive/IT-III/ADP-III require a favorably adjudicated Tier 1/NACI investigation or greater IAW DoDI 5200.46, DoD Investigative and Adjudicative Guidance for Issuing the Common Access Card (CAC), dated 9 Sep 2014, DoDM 1000.13, Vol 1, DoD Identification (ID) Cards: ID Card Lifecycle, dated 23 Jan 2014, and Defense Counterintelligence and Security Agency (DCSA) standards. Before a CAC or NIPRNet access will be granted, a favorable Tier 1/NACI investigation or greater must be on record in Defense Information Security System (DISS), and a favorable Federal Bureau of Investigation (FBI) National Criminal History Check (fingerprint check) on record with DCSA. A CAC may be issued on an interim basis based on a favorable FBI fingerprint check and successful submission of a Tier 1 investigation to DCSA NBIB, and on record in DISS.

NOTE: The above requirements for Non-Sensitive/IT-III/ADP-III positions are for unclassified access and systems only. No classified access will be granted based on the Tier 1 investigation. USTRANSCOM will only process Tier 1 investigations and will not complete any personnel security investigations (Tier 3/Tier 5) for classified access. It is incumbent upon the contractor to have the appropriate investigations completed upon start of the task order.

5.4. Security Clearance and Special Compartmented Information (SCI) Requirements

All positions on this contract/task order, require a minimum of either an interim SECRET granted by the Vetting Risk Operations Center (VROC), or a completed adjudication of SECRET granted by the DoD Consolidated Adjudication Facility (CAF). In addition, some tasks on this contract require access to Sensitive Compartmented Information (SCI). Contractors working directly on tasks requiring access to TS-SCI or TS must have an eligibility determination of TOP SECRET as granted by the Defense Industrial Security Clearance Office (DISCO). Tasks that require collateral TOP SECRET and TOP SECRET/SCI security clearances are outlined in the table below. TS-SCI will not be released to contractor employees without specific release approval of the originator.

Paragraph	Task Area	Restricted System Access	TOP SECRET	SCI
1.4.2.	Joint Deployment and Distribution Enterprise (JDDE) Campaign Planning.		X	4
1.4.3.	Capability Development		X	5

5.5. Facilities Clearance (FCL).

The contractor must have a valid FCL at the SECRET level. FCL procedures and security guidelines for adjudicative requirements are outlined in DOD 5220.22-M. FCLs and interim FCLs must be awarded by the Defense Counterintelligence and Security Agency (DCSA) Facility Clearance Branch.

5.6. Personnel Clearance Validation

Upon contract/task order award, the contactor shall submit the names of contractor personnel to the USTRANSCOM contracting team, who will provide to TCCS-PR for vetting through DISS

or the Defense Information Security System (DISS) to ensure investigative and clearance requirements have been satisfied. This shall be completed before the COR/Trusted Agent (TA) accesses the DOD Trusted Associate Sponsorship System (TASS) and creates CAC applications for contractor personnel. If a contractor's employee does not have the required investigative or security clearance level based on the Government's determination, the contractor's employee will be denied the ability to work in support of this contract/task order.

5.7. Common Access Card Issuance Procedures.

a. For those personnel that do not have the required background investigation (the FSO will make the determination by searching for a valid account for that person in DISS). If a valid account does not exist in DISS, the contracting company must submit to the USTRANSCOM Personnel Security Manager (through the CO or COR), an OF Form 306 (Declaration for Federal Employment), and a SF 85 (questionnaire for Non-Sensitive Positions) it's only sent after the FSO or equivalent reviews it for accuracy.

b. At the same time, the contractor company will coordinate and obtain electronic fingerprinting for their employee. The third-party Company will "electronically" capture the applicant's fingerprints, using the USTRANSCOM (SON, SOI, and ALC). Hardcopy fingerprint cards are not acceptable.

These steps shall be completed before the COR/Trusted Agent (TA) accesses the DOD Trusted Associate Sponsorship System (TASS), to create a CAC application.

Basic U. S. Citizen Contractor CAC Requirements:

Requires access on a continual basis of 6 months or more.

Contract personnel require access to a DoD facility or networks, either on-site or from a remote location.

Users need access to systems for platforms that requires CAC login or user authentication.

Basic Non- U. S. Citizens Contractor CAC Requirements:

Possess legal U. S. residency for a period of 3 or more years with a completed Tier 1 background investigation and fingerprint card. Also meet (as a direct/indirect DoD hire personnel) the investigative requirements for DoD employment as recognized through international agreements pursuant to subchapter 2131 of DoD 1400.25 (reference M).

Possess (as foreign military, employee or contract support personnel), a visit status and security assurance that has been confirmed, documented and processed IAW international agreements pursuant to DoDI 1400.25: Civilian Personnel Management.

CAC Applications:

The CAC applications must have an adjudicated Tier 1, Tier 3 or Tier 5 background investigation posted in DISS, or

An interim CAC may be approved when the contractor employee has a favorable fingerprint, name and criminal records check completed and has either a Tier 1, Tier 3 or Tier 5 background check "open" with DCSA.

The TASS TA will not approve the CAC application in TASS until that TA has verified with a member of USTRANSCOM Protection and Response (TCCS-PR), one of the above requirements.

5.8. Access to Scott Air Force Base or USTRANSCOM Facilities.

Upon receipt of the CAC, permanently assigned contractor personnel located at USTRANSCOM at Scott AFB (SAFB), IL, may obtain the AF 1199 (Restricted Area Badge) if the employee meets the requirements set forth in SAFB Instruction 31-101. This stipulates that personnel who request AF 1199's be assigned physically on SAFB at least four (4) days a week with a desk computer and phone before an AF 1199 will be issued. The Government will provide unrestricted access to facilities, consistent with security clearance and need to know, necessary for the on-site personnel to perform their work IAW the task order. Contractor personnel assigned on-site at USTRANSCOM will wear and display the Restricted Area badge at all times while in Government facilities. Visits to SAFB by contractor personnel who do not possess the CAC will be facilitated by the COR/CO sponsoring the employee through the online base access system.

5.9. Visits by Non-Assigned Contractors to USTRANSCOM/SDDC Buildings

Any visit(s) by contractor personnel not permanently assigned to this task order (i.e., company presidents, company security managers, contractor personnel not permanently assigned at SAFB, etc.) require an electronic visit request be submitted using DISS. DISS visits can be forwarded to the Security Management Office (SMO) code: USTC-SDDC. The visit request shall annotate the task order number in the POC block of the visit request and the name/phone number of either the functional, COR or CO in the phone number block.

5.10. Visits by Permanently Assigned Contractors

Permanently assigned contractor employees on SAFB will require a visit request for the current period of performance posted in DISS to SMO: USTC-CONT. The visit request will annotate the contract number in the POC block of the visit request and the name/phone number of either the functional, COR or CO in the phone number block. Upon in-processing permanently assigned contractors will require a copy of the DD Form 254 for this task order to show the classified access level for this task order and to assist in assigning permissions on restricted area badges.

5.11. Supplemental Notes Regarding Visit Information in DISS

4ersonnel requiring access to Government facilities will properly complete the "Visit Information" block in DISS. Otherwise, contractor employees will be denied access to the facility and classified and/or sensitive information. Also, prime contractors will annotate their contract number and subcontractors will provide the name of their Company, with the prime contract number they are assigned to by the Prime, in the "additional information" block of the Visit table. A valid "Reason for the Visit" must be stated and the "visit access" must not exceed that of the contract.

5.12 Security and Emergency Operations Training

Contractor personnel physically assigned at USTRANSCOM at SAFB shall attend/complete the following training as prescribed by DOD, USTRANSCOM and Air Force Instructions: Annual Security Awareness, OPSEC, DOD Antiterrorism Level I, Active Shooter, Emergency Operations and any Security Stand-down Day Training scheduled by the Commander, USTRANSCOM. Contractor personnel assigned elsewhere shall attend security training established by their respective Government security offices and/or installations.

5.13. Additional Security Conditions.

All contractors assigned to USTRANSCOM on SAFB will complete the contactor in-processing checklist before the start of work on this or any contract/task order in USTRANSCOM. Contractors starting work on a new contract will report to the Protection Service Desk (PSC), located in Building 1900 Breezeway. In-processing includes the following:
Verification of personal Identification
Review of the employee copy of the contract DD-254
Matching information from the DD-254 to the Visitor Notification in DISS
Verification of the contractors Security Clearance in DISS
Brief and sign the individual SF-312 (Security Agreement)
Review of access requirements
Issuance of a Temporary Line Badge (AF-1199) for the facility
Creation of a personnel file
Brief North Atlantic Treaty Organization (NATO) Access

5.14. Derogatory Information.
If the Government notifies the contractor that the employment or the continued employment of any contractor personnel is prejudicial to the interests or endangers the security of the United States of America, that employee shall be removed and barred from the worksite. This includes security deviations/incidents and credible derogatory information on contractor personnel during the course of the task order's period of performance as noted in DISS. Personnel who have incident reports posted in DISS will be denied the ability to support the task order until the issues have been resolved and the incident has been removed in DISS. The contractor shall make any changes necessary in the appointment(s), at no additional cost to the Government. If any incident involves or may involve the mishandling of classified information or a potential Negligent Discharge of Classified Information, the USTRANSCOM Protection and Response office (618-220-6554) will be notified within 24 hours during the normal work week and within 72 hours if the incident occurs over the weekend.

5.15. Accessing NATO Information.
No contractor employee will access NATO information without first being indoctrinated on NATO and having that access recorded in DISS. Any NATO information accessed will be only on SIPRNet. Senders of NATO information will ensure the receiving network is accredited and the receiving point is a Sub-Registry or authorized Control Point. No NATO information will be stored with US classified information. Access to NATO information will be based on need-to-know, appropriate access level, and training. NATO information will not be disseminated to unauthorized users. NATO information will not be printed unless authorized by a USTRANSCOM NATO –Sub-Registry person in TCCS-PR. All printed NATO classified information must be strictly controlled and tracked in a NATO registry. Contact the USTRANSCOM Sub-Registry for additional control measures. In accordance with the NISPOM, Chapter 10-706, NATO briefed personnel will be re-briefed on an annual basis. USTRANSCOM will indoctrinate all on-site contractor employees and document in DISS. Contractor personnel assigned to USTRANSCOM facilities will be NATO briefed and debriefed by USTRANSCOM, with appropriate annotations to DISS. Company FSOs may take responsibility for all NATO refresher briefings per NISPOM paragraph 10-706 and record the date of the annual briefings in DISS.

5.16. Security Debriefing.
Contractor personnel physically working at USTRANSCOM at SAFB, IL, shall complete the out-processing checklist on the last day of the task order or upon termination or reassignment from duties under the current contract or task order. The following closeout tasks will be completed, before the contractor departs:
Review of the contractor's personnel folder
Review and debrief the contractor's SF-312
Debrief anyone with NATO Access
Update and annotate DISS records reflecting the current status of the contractor at USTRANSCOM
Surrender CAC cards (with a copy of the revocation notice from the COR or TA)
Surrender the facility Restricted Area Badge (AF-1199) to the Protection Service Center
Contractor personnel shall have surrendered all Government supplies, materials and equipment to the COR.

5.17. FORCE PROTECTION:
Contractor employees will comply with antiterrorism Force Protection conditions (FPCONs) at the location they are performing work on, whether it is CONUS or OCONUS.

5.18. NOTE TO THE PRIME CONTRACTOR FACILITY SECURITY OFFICER (FSO): The prime contractor will forward the name, address, email address and telephone number of the Company FSO, and backup, to the USTRANSCOM Office of Protection and Response at:
steven.g.stegen.civ@mail.mil

5.19. USTRANSCOM Protection and Response (Industrial Security) Points of Contact:

USTRANSCOM
Attn: TCCS-PR (Steve Stegen or Andrew Daub)
508 Scott Drive
Scott AFB IL 62225

TCCS-PR Approval Authority: Andrew Daub, USTRANSCOM
TCCS-PR Tracking #: USTRANSCOM-TCCS-0XX-22

6.0. Operations Security
OPSEC must be included in contracts to ensure that critical information is protected. Disclosing this information to the adversary could potentially affect mission success and cause harm to military members, civilians, and contractors and their families. OPSEC is a process used to protect unclassified sensitive information from exploitation by an adversary. Sensitive unclassified information—which is also referred to as critical information or critical program information (CPI)—is defined as information that is not classified but which needs to be protected from unauthorized disclosure. Examples are information labeled "Controlled Unclassified Information (CUI)," proprietary information, contractor sensitive information, limited distribution information, and personally identifiable information (PII).

6.1. Operations Security Requirements

The prime contractor and all subcontractors shall provide protection for sensitive unclassified information in order to limit unauthorized disclosures of critical information. The prime contractor and all subcontractors shall employ the countermeasures listed below to protect that information. These OPSEC requirements will be in effect throughout the life of the procurement from award through the conclusion of services at the end of the period of performance or other procurement termination. In any case where uncertainty or ambiguity regarding OPSEC measures exists, the contractor shall consult the requirements or contracting office's OPSEC coordinator as soon as possible.

6.2. Countermeasures to Unauthorized Disclosure of Critical Information

Countermeasures are required to negate the susceptibility of critical information to exploitation by an adversary or competitor. The contractor shall protect all critical information listed in a manner appropriate to the nature of the information, including use of the necessary countermeasures as listed below applicable to specific items:

- Encryption with a password of electronically stored critical information.
- Encryption or password protection of e-mail containing critical information.
- Storage of hard copy critical information, optical media, and external hard drives in locked containers when not in use.
- Transmission of critical information to the minimum set of recipients with a need to know.
- Immediate and appropriate destruction in a manner precluding reconstruction of all critical information no longer needed under this contract.
- Restricting verbal discussion of critical information to venues and circumstances that prevent the monitoring and interception of the discussion by unauthorized personnel.
- Refraining from the use of unencrypted telephones to transmit critical information.
- Refraining from the use of foreign postal systems to ship critical information.
- Promptly retrieving documents containing critical information printed on printers accessible by persons without a need to know the critical information.
- Use of cover pages or other appropriate means to prevent the viewing of critical information by unauthorized persons.
- Refrain from including critical information in contract and budget documents, presentations, press releases, and other publications to that which is essential to the performance of this requirement.
- The contractor shall notify the COR and USTRANSCOM security office immediately of all known and suspected compromises of critical information. If the COR cannot be reached, the contractor shall notify the supported command duty officer if after normal work hours.

REFERENCES:

Defense Electronic Libraries:

Acquisition Notes: http://acqnotes.com
Assist – Quick Search: http://quicksearch.dla.mil
Official Website of the Joint Chiefs of Staff (JCS): https://www.jcs.mil/
Defense Acquisition University (DAU): https://www.dau.mil
Department of Defense: http://www.esd.whs.mil/dd/dod-issuances/
Federal Registry: https://www.federalregister.gov/
Joint Electronic Library: https://www.jcs.mil/Doctrine/
USTRANSCOM: https://ww2.ustranscom.mil/FP_2018/fp_index.cfm
Security Regulation Guidance: http://www.dtic.mil/whs/directives/corres/pub1.html
Federal Information Processing Standards (FIPS) and National Institute of Standards and Technology (NIST): https://csrc.nist.gov/publications
Military Standards (MIL-STD): https://www.dau.mil/
Committee on National Security Systems (CNSS):
https://www.cnss.gov/CNSS/issuances/Instructions.cm
Institute of Electrical and Electronics Engineers (IEEE) Publications:
https://www.ieee.org/publications_standards/index.html
Governing Guidance and Directives:
American National Standards Institute (ANSI)/Electronic Industries Alliance (EIA) 748: Earned Value Management, current edition
CJCS Instruction 5123.01H, Charter of the Joint Requirements Oversight Council (JROC) and Implementation of the Joint Capabilities Integration and Development Systems (JCIDS), August 31, 2018
CJCS Instruction 6510.01F, Information Assurance (IA) and Support to Computer Network Defense (CND), June 9, 2015
CJCSM 3213.02D, Joint Staff Alternative Compensatory Control Measures (ACCM) Program Management Manual (Limited Distribution)
CJCSM 6510.01B, Cyber Incident Handling Program, 10 July 2012
Data Item Management-81861, Data Item Description: Integrated Program Management Report (IPMR), June 20, 2012
DD Form 254, Contract Security Classification Specification, November 1, 2017
Defense Federal Acquisition Regulation Supplement, current edition
DOD 5200.08, Security of DoD Installations and Resources and the DoD Physical Security Review Board (PSRB), Change 3, November 20, 2015
DOD Instruction 5220.22, National Industrial Security Program, May 1, 2018
DODM 6025.18, Implementation of The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule in DoD Health Care Programs, March 13, 2019
DOD Instruction 8500.01, Cybersecurity, Change 1, October 7, 2019
DOD Instruction, 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT), Change 2, July 28, 2017
DOD Directive 5230.25, Withholding of Unclassified Technical Data from Public Disclosure, December 28, 2016
DOD Instruction 8320.02, Data Sharing, in a Net Centric Department of Defense, August 5, 2013

DOD Instruction 1100.22, Policy and Procedures for Determining Workforce Mix, Change 1, December 1, 2017
DOD Instruction 2000.12, DoD Antiterrorism (AT) Program, Change 3, May 8, 2017
DOD Instruction O-2000.16, DoD Antiterrorism (AT) Program Implementation: DoD AT Standards, Volume 1, November 17, 2016, with C3 May 7, 2021
DOD Instruction O-2000.16, DoD Antiterrorism (AT) Program Implementation: DoD Force Protection Condition (FPCON) System Volume 2, May 8, 2017, with C1 May 8, 2017
DOD Instruction 5025.13, DOD Plain Language Program, January 23, 2020
DOD Instruction 5200.02, "Personnel Security Program," September 9, 2014
DOD Instruction 8330.01, "Interoperability of Information Technology (IT), Including National Security Systems (NSS)," December 18, 2017
DOD Instruction 8500.01, "Cybersecurity," March 14, 2014
DOD Instruction 8510.01, "Risk Management Framework (RMF) for DOD Information Technology (IT)," July 28, 2017
DOD Instruction 8520.02, "Public Key Infrastructure (PKI) and Public Key (PK) Enabling," May 24, 2011
DOD Instruction 8551.01, "Ports, Protocols, and Services Management (PPSM)", July 27, 2017
DOD Instruction 8582.01, "Security of Unclassified DOD Information on Non-DOD Information Systems," October 27, 2017
DOD Manual 1000.13, Volume 1, "DOD Identification (ID) Cards: ID Card Life- Cycle," January 23, 2014, with C1 July 28, 2020
DOD Manual 5200.01, Volume 1, "DOD Information Security Program: Overview, Classification, and Declassification," February 24, 2012, with C2, July 28, 2020
DOD Manual 5200.01 Volume 2, "DOD Information Security Program: Marking of Classified Information," March 19, 2013, with C4 July 28, 2020
DOD Manual 5200.01 Volume 3, "DOD Information Security Program: Protection of Classified Information," March 19, 2013, with C3, July 2020
DODI 5200.48, "Controlled Unclassified Information," 6 March 2020
DOD 5200.08-R, Change-1, DoD Physical Security Program, May 27, 2009
DFARS 252.205-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting
DOD Manual 5200.02, "Procedures for the DOD Personnel Security Program (PSP)," April 3, 2017, with C1 October 29, 2020
DOD Manual 5220.22, Volume 3, "National Industrial Security Program: Procedures for Government Activities Relating to Foreign Ownership, Control, or Influence (FOCI)," April 17, 2014, with C1 August 5, 2020
DOD Standard MIL-STD-881C, "Work Breakdown Structures (WBS) for Defense Materiel Items," October 3, 2011
Office of Management and Budget Circular A-11, "Preparing, Submitting, and Executing the Budget," current edition
USTRANSCOM Instruction 31-02, "Security Classification Guide," April 6, 2018
USTRANSCOM Instruction 5200.08, "Operations Security," 18 June 2021
USTRANSCOM Instruction 33-1, "Information Systems Security Education, Training, and Awareness Program," March 27, 2017
USTRANSCOM Instruction 33-48, "Data Management Policy and Responsibilities," February 16, 2016

USTRANSCOM Instruction 33-58, “Cyber Workforce Management,” February 26, 2016
Scott Air Force Base: AF Instruction 31-101_AMC, January 4, 2014
FIPS 199, “Standards for Security Categorization of Federal Information and Information Systems,” February 2004
FIPS 200, “Minimum Security Requirements for Federal Information and Information Systems,” March 2006
NIST SP 800-18 Revision 1, “Guide for Developing Security Plans for Federal Information Systems” February 2006
NIST SP 800-30 Revision 1, “Guide for Conducting Risk Assessments,” September 2012
NIST SP 800-37 Revision 2, “Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy,” June 5, 2014
NIST SP 800-53, Revision 4, “Security and Privacy Controls for Federal Information Systems and Organizations,” January 22, 2015
NIST SP 800-53A Revision 4, “Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans,” December 18, 2014
NIST SP 800-60 Volume 1, Revision 1, “Guide for Mapping Types of Information and Information Systems to Security Categories,” August 2008
NIST SP 800-61 Revision 2, “Computer Security Incident Handling Guide,” August 2012
CNSS Instruction 1253, “Security Categorization and Control Selection for National Security Systems,” March 27, 2014
12207.0-1996 IEEE/EIA Standard Industry Implementation of International Standard ISO/IEC 12207: 1995 (ISO/IEC 12207) Standard for Information Technology Software Life Cycle Processes. Superseded by 12207-2008 – Standard for Information Technology – Software Life Cycle Processes
12207.1-1997 - Industry implementation of International Standard ISO/IEC 12207: 1995. (ISO/IEC 12207) Standard FOR Information Technology - Software Life Cycle Processes - Life Cycle Data superseded by: 15289-2017: 15289-2017 - ISO/IEC/IEEE Draft International Standard - Systems and software engineering -- Content of life-cycle information items (documentation)
Executive Order (E.O.) 13691 of February 13, 2015. Promoting Private Sector Cybersecurity Information Sharing

APPENDICES:

1. **ACRONYMS**
2. **NON-DISCLOSURE AGREEMENT (NDA) FOR CONTRACTOR EMPLOYEES**
3. **PLANNING, PROGRAMMING, BUDGETING, AND EXECUTION (PPBE) NDA FOR CONTRACTOR EMPLOYEES**

Appendix 1

ACRONYMS

Acronym	Definition
ADP	Automated Data Processing
AJA	Annual Joint Assessment
AMC	Air Mobility Command
CAC	Common Access Card
CGA	Capabilities Gap Assessment
CGP	Corporate Governance Process
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CO	Contracting Officer
COI	Community of Interest
CCMD	Combatant Command
CCP	Combatant Command Campaign Plan
COR	Contracting Officer's Representative
CPA	Campaign Plan Assessment
CP-GDD	Campaign Plan for Global Deployment and Distribution
CSF	Command Strategy Forum
DEERS	Defense Enrollment Eligibility Reporting System
DISS	Defense Information Security System
DISCO	Defense Industrial Security Clearance Office
DLA	Defense Logistics Agency
DOD	Department of Defense
DOTMLPF-P	Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities, and Policy
DTS	Defense Transportation System
eCMRA	Electronic Contractor Manpower Reporting Application
FCL	Facilities Clearance Level
FCP	Functional Campaign Plan
FTE	Full Time Equivalent
FCP-GDD	Functional Campaign Plan for Global Deployment and Distribution
GCP	Global Campaign Plan
GDA	Global Distribution Assessment
GEF	Guidance for the Employment of the Force
GO/FO	General Officer/Flag Officer
IAW	In Accordance With
IPL	Integrated Priority List
IPR	In-Process Reviews
IT	Information Technology
IMO	Intermediate Military Objective
JCA	Joint Capability Area
JCIDS	Joint Capability Integration Development System

JDD	Joint Deployment and Distribution
JDDE	Joint Deployment and Distribution Enterprise
JECC	Joint Enabling Capabilities Command
JROC	Joint Requirements Oversight Council
JS	Joint Staff
JSAP	Joint Staff Action Package
JSCP	Joint Strategic Capability Plan
KM/DS	Knowledge Management/Decision Support
LOE	Line of Effort
MSC	Military Sealift Command
MSR	Monthly Status Report
NATO	North Atlantic Treaty Organization
NIPRNet	Non-secure Internet Protocol Router Network
ODC	Other Direct Costs
OSD	Office of the Secretary of Defense
PPBE	Planning, Programming, Budgeting and Execution
PSC	Protection Services Center
PWS	Performance Work Statement
RAPIDS	Real-Time Automated Personnel Identification System
RDT&E	Research, Development, Test, and Evaluation
SCI	Secret Compartmentalized Information
SDDC	Surface Deployment and Distribution Command
SIPRNet	Secure Internet Protocol Router Network
SMO	Security Management Office
TA	Trusted Agent
TASS	Trusted Associate Sponsorship System
TCC	Transportation Component Command
TCJ5/J4	USTRANSCOM Strategic Plans, Policy, and Logistics Directorate
TDP	Theater Distribution Plans
TMT	Task Management Tool
TOMP	Task Order Management Plan
TPP	Theater Posture Plans
UCP	Unified Command Plan
USTRANSCOM	United States Transportation Command

Appendix 2

NONDISCLOSURE AGREEMENT AND AGREEMENT TO DISCLOSE POTENTIAL CONFLICTS OF INTEREST FOR CONTRACTOR EMPLOYEES ON USTRANSCOM CONTRACTS

NOTE: This Agreement is a standard agreement designed for use by contractor (including sub-contractor) employees assigned to work on USTRANSCOM contracts. Its use is designed to protect non-public Government information from disclosure, identify potential conflicts of interest, and prevent violations of federal statutes/regulations. The restrictions contained in this agreement also serve contractors by promoting compliant behavior that keeps contractors eligible to compete for Government contracts. In addition to the potential impact on future business opportunities, failure to abide by this agreement could result in administrative, civil, or criminal penalties specified by statute or regulation.

1. I, _____, currently an employee of _____, hereby agree to the terms and conditions set forth below.

2. I understand that I may have access to confidential business information, contractor bid or proposal information (as defined by FAR 3.104-1), and/or source selection information (as defined by FAR 2.101) either for contract performance, as a result of working in a USTRANSCOM facility, or of working near USTRANSCOM personnel, contractors, visitors, etc. I fully understand that such information is sensitive and must be protected in accordance with 41 US Code Section 423 and FAR SubPart 3.1.

3. In the course of performing under contract/order # _____ or some other contract or sub-contract for USTRANSCOM, I agree to:

a) Use only for Government purpose any and all confidential business information, contractor bid or proposal information, and/or source selection sensitive information to which I am given access. I agree not to disclose "non-public information" by any means (in whole or in part, alone or in combination with other information, directly, indirectly, or derivatively) to any person except to a US Government official with a need to know or to a non-Government person (including, but not limited to, a person in my company, affiliated companies, sub-contractors, etc.) who has a need to know related to the immediate contract/order, has executed a valid form of this non-disclosure agreement, and receives prior clearance by the Contracting Officer. All distribution of the documents will be controlled with the concurrence of the Contracting Officer.

b) "Non-public information," as used herein includes trade secrets; confidential or proprietary business information (as defined for Government employees in 18 USC 1905); advance procurement information (future requirements, acquisition strategies, statements of work, budget/program/planning data, etc.); source selection information (proposal rankings, source selection plans, contractor bid or proposal information); information protected by the Privacy Act (social security numbers, home addresses, etc.); sensitive information protected from release under the Freedom of Information Act (pre-decisional deliberations, litigation materials, privileged

material, etc.); and information that has not been released to the general public and has not been authorized for such release (as defined for Government employees in 5 CFR 2635.703).

c) Not use such information for any non-Governmental purposes, including, but not limited to, the preparation of bids or proposals, or the development or execution of other business or commercial ventures.

d) Store the information in such a manner as to prevent inadvertent disclosure or releases to individuals who have not been authorized access to it.

4. I understand that I must never make an unauthorized disclosure or use of confidential business information, contractor bid or proposal information, and/or source selection sensitive information unless:

a) The information has otherwise been made available without restriction to the Government, to a competing contractor or to the public.

b) The Contracting Officer determines that such information is not subject to protection from release.

5. I agree that I shall not seek access to "non-public information" beyond what is required for the performance of the services I am contracted to perform. I agree that when I seek access to such information, attend meetings, or communicate with other parties about such information, I will identify myself as a contractor. Should I become aware of any improper or unintentional release or disclosure of "non-public information," I will immediately report it to the Contracting Officer in writing. I agree that I will return all forms (including copies or reproduction of original documents) of any "non-public information" provided to me by the Government for use in performing my duties to the control of the Government when my duties no longer require this information.

6. Because the Government expects unbiased judgment and recommendations from contractors performing work under its contracts and orders, I agree to advise the Contracting Officer of any actual or potential personal conflicts of interest I may have related to any work I perform under this contract/order with the government. Personal conflicts of interest include any matter in which I or my spouse, minor child, or household member has a financial interest. A financial interest is any interest in, or affiliation with, a prime contractor, subcontractor to a prime contractor, any offerors, or any prospective subcontractor to any offeror for the program, contract, or other matter for which I am performing a support task under this contract. The financial interest can take the form of any ownership interest (including but not limited to: stock; ownership of bonds; vested or unvested retirement benefits; a loan or other financial arrangement that is other than an arm's-length transaction; employment, or an arrangement concerning prospective employment including negotiations therefore; or any non arm's length loan, any gift from or other non arm's length financial arrangement with any person who is directly communicating with the government on behalf of the prime contractor, subcontractor, or any prospective subcontractor or offeror). With respect to conflict of interest disclosures required under this agreement, a financial interest in, or affiliation with, the prime contractor that is my employer under this contract does not have to be

disclosed to the Contracting Officer. If any potential conflicts of interest, real or otherwise, do present themselves, then I shall immediately disclose the pertinent information to the Contracting Officer.

By signing below, I certify that I have read and understand the terms of this Non-Disclosure Agreement and Agreement to Disclose Potential Conflicts of Interest, and voluntarily agree to be bound by its terms.

_____ _____

Signature of Contractor Employee Date

_____

Printed Contractor Employee Name

_____ _____

Government Contracting Officer's Representative Date

Appendix 3

PLANNING, PROGRAMMING, BUDGETING, AND EXECUTION (PPBE) NONDISCLOSURE AGREEMENT FOR CONTRACTOR EMPLOYEES ON USTRANSCOM CONTRACTS

NOTE: This Agreement is designed for use by contractor (including sub-contractor) employees who may require access to PPBE information in the performance of their work on USTRANSCOM contracts. Its use is designed to protect non-public Government PPBE information from disclosure and prevent violations of federal statutes/regulations. Failure to abide by this agreement could result in administrative, civil, or criminal penalties specified by statute or regulation.

1. I, _____, currently an employee of _____, hereby agree to the terms and conditions set forth below.

2. I understand that in the performance of this contract, I may have access to Planning, Programming, Budgeting and Execution (PPBE) documents and information, as defined in DOD Directive 7045.14

3. I agree not to use, discuss, divulge, or disclose any such information or data to any person or entity except those persons directly concerned with the use or performance of this contract. I have been advised that the unauthorized disclosure, use, or negligent handling of the information by me could cause irreparable injury to the Government.

4. I understand that the United States Government may seek any remedy available to it to enforce this Agreement, including, but not limited to, application for a court order prohibiting disclosure of information in breach of this agreement. Court costs and reasonable attorney fees incurred by the United States Government may be assessed against me if I lose such action.

By signing below, I certify that I have read and understand the terms of this Non-Disclosure Agreement and voluntarily agree to be bound by its terms.

_____ _____
Signature of Contractor Employee Date

_____
Printed Contractor Employee Name

_____ _____
Government Contracting Officer's Representative Date