U.S. General Services Administration
Federal Acquisition Service
Northeast and Caribbean Region

PERFORMANCE WORK STATEMENT (PWS)
FOR
U.S. SOUTHERN COMMAND (USSOUTHCOM)
ENTERPRISE INFORMATION TECHNOLOGY SERVICES SUPPORT CONTRACT
(EITSSC)

Issued By:

U.S. General Services Administration
Federal Acquisition Service, Region 2
Attn: Charles Ade, Contracting Officer
Phone: 347-525-5151
Email: charles.ade@gsa.gov

~~RFQ /~~ ITSS task **#** ID02140034

(Version 3.0, dated 06/07/2016– see change log at end of document)

Table of Contents

Table of Contents 2
PART 1 14
1. GENERAL 15
1.1 Description of Services/Introduction 15
1.2 Background 15
1.3 Objectives 16
1.4 Scope 17
1.5 Period of Performance 17
1.6 General Information 17
1.6.1 IT Life Cycle Execution and Quality Control 18
1.6.2 Quality Assurance 18
1.6.3 Recognized Holidays 18
1.6.4 Hours of Operation 18
1.6.5 Place of Performance 19
1.6.6 Type of Contract 20
1.6.6.1 Additional Hours greater than 40 Hours Per Week. 20
1.6.7 Security Requirements 20
1.6.7.1 Physical Security 20
1.6.7.2 Key Control 20
1.6.7.2.1 Lost Keys 21
1.6.7.2.2 Use of Keys by Other Persons 21
1.6.7.3 Lock Combinations 21
1.6.7.4 Reporting Security Incidents 21
1.6.8 Special Qualifications 21
1.6.8.1 Qualified Contractor Support Personnel 21
1.6.8.2 Personnel Resumes 22
1.6.8.3 Computing Environment, Technical, and Functional Area Training of Contractor Personnel 22
1.6.8.4 Information Assurance Certification of Contractor Personnel 24
1.6.8.5 Driver Qualifications 26

1.6.8.6 DoD/USSOUTHCOM Required Training 26
1.6.8.6.1 Training on Combatting Trafficking in Persons 26
1.6.9 Post Award Conference/Quarterly Progress Review Meetings 27
1.6.9.1 Periodic Progress, Status, and Management Report 27
1.6.10 Contracting Officer Representative (COR) 27
1.6.10.1 Assistant Contracting Officer Representatives (ACORs) 28
1.6.11 Contractor Key Personnel 29
1.6.12 Identification of Contractor Personnel 29
1.6.13 Contractor Travel Expense Reimbursement 30
1.6.13.1 Theater and Country Clearances 30
1.6.13.2 OCONUS Travel Security and Other Related Requirements 31
1.6.13.2.1 ISOPREP Requirements Details. 31
1.6.14 Other Direct Costs 32
1.6.15 Data Rights 32
1.6.16 Organizational Conflict of Interest 33
1.6.16.1 Non-Disclosure Agreements 33
1.6.17 War Risk Insurance 33
1.6.18 Phase In/Phase Out Periods 34
1.6.19 Local Nationals 34
1.6.19.1 Local National Personnel – Adherence to Local Country Laws 34
1.6.20 Permanent Change of Station (PCS) to JTF-Bravo, JTF-GTMO or a SCO 34
1.6.20.1 Household Goods and Privately Owned Vehicles (POVs) to JTF-GTMO 35
1.6.20.2 Use of Government Facilities and Services at JTF-GTMO 35
1.6.20.3 Use of Government Facilities and Services at JTF-Bravo 35
1.6.20.4 Travel to JTF-GTMO 35
1.6.20.5 Personnel Vacancy for JTF-Bravo, JTF-GTMO, or SCOs 35
1.6.21 Access to Strategic or Fiscal Planning Government Systems 35
1.6.22 Employment Eligibility 35
PART 2 37
2. DEFINITIONS AND ACRONYMS 37
2.1 Definitions 37
2.2. Acronyms 43

PART 3 51
3. GOVERNMENT FURNISHED ITEMS AND SERVICES 51
3.1. Services 51
3.2 Facilities 51
3.3 Utilities 51
3.4 Government Furnished Equipment (GFE) 51
3.4.1 Administrative Support Equipment 51
3.4.2 GFE Information Technology (IT) Equipment 52
3.4.3 Contractor Acquired Property 52
3.4.4 Replacement of GFE 52
3.4.5 Disposition of Replaced / Unserviceable Parts 52
3.5 Materials and Information 53
3.6. Organizational Information 53
PART 4 54
4. CONTRACTOR FURNISHED ITEMS AND RESPONSIBILITIES 54
4.1 General 54
4.2 Facility Clearance, Employee Security Clearances, and Related Requirements 54
4.2.1 Visit Certifications 55
4.2.2 Notification of Personnel working on this Task Order 56
4.3. Materials to include Drawings, Diagrams, Plans, Procedures, Policies, and Other Systems Documents 56
4.3.1 Classified Material 57
4.3.2 Information Systems Security 57
4.3.2.1 Safeguarding public key infrastructure (PKI) Tokens 57
4.4. Equipment 57
4.5 Drug Testing 57
4.6 Polygraph Testing 57
4.7 Medical Insurance for Work at JTF-GTMO 58
4.8 Common Access Cards and SIPRNET Tokens for Personnel working on this Task Order 58
PART 5 59
5 Specific Tasks 59
5.1 Basic Services 62

5.1.1 Enterprise IT Service Strategy and Planning 65
5.1.1.1 Phase-In Plan for Assumption of Operations and Maintenance of USSOUTHCOM Communications Systems and Deprecation of TCSC, JTF-Bravo, and JTF-GTMO SIPRNET and NIPRNET Networks in the AOR. 65
5.1.1.1.1 IT Service Corrective Action Planning 65
5.1.1.2 Joint Information Environment (JIE) Transformation Planning 66
5.1.1.2.1 Data Center Consolidation Planning 66
5.1.1.2.2 Software-as-a-Service Planning 67
5.1.1.2.3 Active Directory Planning. 67
5.1.1.2.4 Identity and Access Management (IdAM) Planning 67
5.1.1.2.5 Client Modernization (CM) Planning 68
5.1.1.2.6 SC Single Security Architecture Planning 68
5.1.1.2.7 Unified Capabilities Planning 68
5.1.1.3 New Communications Systems Capability Planning 68
5.1.1.3.1 New Requirements Impacts to Service Operations. 69
5.1.1.3.2 Facility Site Analysis 69
5.1.1.3.3 VSAT Site Survey and Installation Plan 69
5.1.1.3.3.1 VSAT Permissions 69
5.1.2 Service Design 70
5.1.2.1 Design for Deprecation all Non-SC HQ SIPRNET and NIPRNET Networks. 70
5.1.2.1.1 IT Service Corrective Action Service Design 70
5.1.2.2 Joint Information Environment Design 70
5.1.2.2.1 Data Center Consolidation Design 70
5.1.2.2.2 Software as a Service (SaaS) Design 71
5.1.2.2.3 Active Directory Design 71
5.1.2.2.4 Identity and Access Management (IdAM) Service Design 71
5.1.2.2.5 Client Modernization Design 71
5.1.2.2.6 SC Single Security Architecture (SSA) Design 71
5.1.2.2.7 Unified Capabilities Design 71
5.1.2.3 New Communications Systems Capability Design 71
5.1.2.4 Cybersecurity In the Service Design Phase 72
5.1.3 IT Service Transition 72

5.1.3.1 Deprecation of SIPRNET and NIPRNET Networks - Service Transition. 73
5.1.3.1.1 IT System Corrective Action Service Transition 73
5.1.3.2 Joint Information Environment Transition 73
5.1.3.2.1 Data Center Consolidation Transition 74
5.1.3.2.2 Software-as-a-Service Transition 74
5.1.3.2.3 Active Directory Transition 74
5.1.3.2.4 Identity and Access Management (IdAM) Transition 74
5.1.3.2.5 Client Modernization (CM) Transition 74
5.1.3.2.6 SC Single Security Architecture Transition 74
5.1.3.2.7 Unified Capabilities Transition 74
5.1.3.3 New Communications Systems Capability Transition 75
5.1.4 Service Operations 75
5.1.4.1 Service Operations and Maintenance Plan 75
5.1.4.2 Service Desk Services/Tier 1 Service 76
5.1.4.2.1 Incident and Service Request Ticketing System 77
5.1.4.2.2 Service Desk User Collaboration Tools 77
5.1.4.2.2.1 Frequently Asked Questions 77
5.1.4.2.3 Initial Response to Incidents 77
5.1.4.2.4 User Application or IT Tools Support 77
5.1.4.2.5 Very Important Person (VIP) and Joint Operations Center and Crises Action Center Support 78
5.1.4.2.6 Prioritized Incident Management Process 78
5.1.4.2.7 Customer Portable Asset Tracking and Control 78
5.1.4.2.8 Customer Service Desk Visitor Database Maintenance and Support 78
5.1.4.2.9 Security Cooperation Office (SCO) Tier 1 Support 79
5.1.4.2.10 Service and Network Monitoring 80
5.1.4.2.11 Service Catalog 81
5.1.4.3 Tier 2 Technical Support 81
5.1.4.3.1 Desktop Integration and Testing 81
5.1.4.3.2 Personal Computer Operating Systems and Applications 81
5.1.4.3.1.1 Desktop Baseline Permutations 81
5.1.4.3.2 New Device Installation and Integration 82

5.1.4.3.3 Hardware Repair 82
5.1.4.3.4 Data-at-Rest 82
5.1.4.4 Tier 3 Support 82
5.1.4.4.1 Server Farm Systems Administration 82
5.1.4.4.1.1 System Administration 82
5.1.4.4.1.2 User Access 83
5.1.4.4.1.2.1 Verification of User eligibility for Access 83
5.1.4.4.1.3 Scripting Management 83
5.1.4.4.2 Database Management and Administration 84
5.1.4.4.2.1 Operate, Maintain, and Modify Databases 84
5.1.4.4.2.2 Database Analysis, Maintenance, and Corrective Action 84
5.1.4.4.3 Theater Information Assurance Security Stack Maintenance 84
5.1.4.4.3.1 Antivirus Update Support 84
5.1.4.4.4 Network Management Support 84
5.1.4.4.4.1 Network IP Range Management 85
5.1.4.4.5 Domain Name Service (DNS) Support 85
5.1.4.4.6 VPN Access and Gateways Support 85
5.1.4.4.7 Hoteled Systems Installation Support 85
5.1.4.4.8 Data Replication in Support of Continuity of Operations (COOP) (DRSC) Operations and Maintenance 86
5.1.4.4.9 Voice System Operations and Maintenance 86
5.1.4.4.9.1 Telecommunications Company (Telco) Telephone Line and Circuit Management 86
5.1.4.4.9.2 Voice Over IP Systems 86
5.1.4.4.9.3 Telephone System Information Directory 86
5.1.4.4.10 IT System Usage Logs 86
5.1.4.4.10 Technical Control Facility /Network Operations Centers/Remote Hub Node Facilities or Data Centers 87
5.1.4.4.10.1 COMSEC Equipment Operations and Maintenance 87
5.1.4.4.10.2 DISA Node Site Coordinator 87
5.1.4.4.11 Video Teleconferencing Services (VTC, Briefing and Display Systems, and Conference Room Support) 87
5.1.4.4.11.1 Public Address Systems Support 88

5.1.4.4.11.2 SC HQ IP Television 88
5.1.4.4.12. Satellite Communications Support 88
5.1.4.4.12.1 MILSTAR Terminal 88
5.1.4.4.12.2 Very Small Aperture Terminal (VSAT) Terminals 88
5.1.4.4.12.2.1 VSAT Hub Services and Network Management 89
5.1.4.4.13 Cable Infrastructure Support 89
5.1.4.4.13.1 Cable Infrastructure Support at Department of State Sites 89
5.1.4.4.14 Global Command and Control Systems-Joint (GCCS-J) Systems Operations and Maintenance 89
5.1.4.4.15 MNIS System Common Operational Picture (COP) Support 90
5.1.4.4.15.1.Common Operational Picture (COP) System Administrator Support 90
5.1.4.4.15.2 Cooperating Sensor Information Integration (CSII) Maintenance Support 90
5.1.4.4.15.3 CSII Integration Support 90
5.1.4.4.15.4 CSII Sensor Integration 91
5.1.4.5 SOUTHCOM Theater Network Coordination Center (TNCC) 91
5.1.4.6 Life Cycle Replacement or Integration of Hardware or Software 91
5.1.5 Minimum Performance Requirements 92
5.1.5.1 Minimum Performance Requirements Formulas and Definitions 92
5.1.6. Key Performance Indicators (KPIs) 93
5.1.6.1 System Resource Utilization KPIs 93
5.1.6.2 Capacity Management KPIs 93
5.1.6.3 Availability Management KPIs 94
5.1.6.4 Information Assurance Management KPIs 94
5.1.6.5 Bandwidth Metrics 95
5.1.7 Continuous Process Improvement 95
5.1.7.1 Quality Control Audits 95
5.1.7.2 Monthly Analysis of Communications Status (COMSTAT) Network Service Call Report, Service Desk Reports, Logs and KPIs. 95
5.1.7.3 Process Improvement Working Group 96
5.1.8. Reserved. 96
5.1.9 Software Engineering and Integration/ Application Development Life Cycle Support Activities 96

5.1.9.1 Existing Web Application Life Cycle Support 96
5.1.9.1.1 Existing Application – SC Baseline Compliance 97
5.1.9.1.2 JDIMS Application Baseline Documentation and Software Re-Engineering 97
5.1.9.2 New Application Development 97
5.1.9.2.1 SEI Policy Compliance 97
5.1.9.2.1.1 Custom Application Development Model 98
5.1.9.2.2 New Application Development using Ozone Widget Framework (OWF) - Option 98
5.1.9.3 Application Hosting – Cloud Hosted Services and Hoteling Services 98
5.1.10 IT Systems Support Services (ITSSS) 98
5.1.10.1.1 Program Management Support 99
5.1.10.1.1.1 Contract Management Specialist Support 99
5.1.10.1.1.2 Finance and Budget Office Support 99
5.1.10.1.1.3 Microsoft Enterprise Project Management Technical Support 100
5.1.10.1.2 Cybersecurity Policy and Defensive Cyber Operations 100
5.1.10.1.2.1 Level 1 Support Services. 101
5.1.10.1.2.1.1 USCYBERCOM (USCC) Orders, Directives, Vulnerability Alerts, Bulletins and Technical Advisories 101
5.1.10.1.2.1.2 Security Technical Implementation Guides (STIGS) 101
5.1.10.1.2.1.3 Cybersecurity Assessments 101
5.1.10.1.2.1.4 Wireless Device Scanning 101
5.1.10.1.2.1.5 Vulnerability Scans and Checks 101
5.1.10.1.2.1.6 Web Content Filtering and Monitoring 102
5.1.10.1.2.1.7 Cybersecurity Monitoring Support 102
5.1.10.1.2.1.8 Training and Certification of Personnel with Elevated Rights 102
5.1.10.1.2.1.9 Tracking, Reporting and Executing Corrective Acton Procedures for Classified Message Incidents 102
5.1.10.1.2.1.10 Cybersecurity Incident Response Analysis / Attack Sensing and Warning Support. 103
5.1.10.1.2.1.10.1 Cybersecurity Forensics Support - Option 103
5.1.10.1.2.1.11 Network Security Event Log 103
5.1.10.1.2.1.12. Communications Security (COMSEC) Support 103
5.1.10.1.2.1.14 Accreditation Packages 104

5.1.10.1.3 Configuration Management....104
5.1.10.1.3.1 Configuration Control and Change Board....104
5.1.10.1.3.2 System Documentation - Approved Baseline Documentation....104
5.1.10.1.3.3 Systems Installation Drawings....104
5.1.10.1.3.4 Physical Configuration Audit....105
5.1.10.1.4 Property Book Office/Warehouse and Acquisition Support....105
5.1.10.1.4.1 Procurement Support....105
5.1.10.1.4.2 Accomplish Purchase Order Execution....105
5.1.10.1.4.3 Contractor Life Cycle Procurement of Hardware, Software, Warrantees and Spare Parts....106
5.1.10.1.4.4 Inventory of Spare Parts, Consumable, Material and Re-order Point Levels....107
5.1.10.1.4.5 Licenses and Warranties....108
5.1.10.1.4.6 Excess Materials....108
5.1.10.1.4.7 Service Desk Database Update....108
5.1.10.1.4.8 Government Property Book Officer (PBO) Liaison ...1085.1.10.1.5 Logistics Support 109
5.1.10.1.5.1 Department of State Certified Warehouse - Option....109
5.1.10.1.5.2 Packaging, Packing and Shipping....109
5.1.10.1.5.3 Transportation....109
5.1.10.1.5.3.1 Coordination of Shipping for Overseas Shipments....109
5.1.10.1.5.3.2 Shipping to US Embassies....110
5.1.10.1.5.3.3 Escort of Equipment in Department of State Controlled Access Areas....110
5.1.10.1.5.4 VSAT Logistics....110
5.1.10.2 IT User Support Services....110
5.1.10.2.1 Sustainment Training....110
5.1.10.2.1.1 Training Facilities....111
5.1.10.2.1.2 Ad-Hoc Training Material....111
5.1.10.2.1.3 Training Material Maintenance....111
5.1.10.2.1.4 Specialized Multinational Training....111
5.1.10.2.2. Multi-National Information Sharing (MNIS) User Support....111
5.1.10.2.3 Global Command and Control Systems-Joint (GCCS-J) J6 User Support....112
5.1.10.2.4 Reserved....113

5.1.10.2.5. CSII User Support 113
5.1.10.2.5.1 CSII User Access Control 113
5.1.10.2.6 SharePoint and APAN Web Portal Support 113
5.1.10.3 Consultants and OEM Support Services 113
5.1.10.3.1 Specialized or OEM Product Consulting Services 114
5.1.10.3.2 Consultants or OEM Service Operations Technical Support 114
5.1.11 Other Required Support Colombia, JTF-Bravo, JTF-GTMO 114
5.1.11.1 JTF-Bravo Unique Support 114
5.1.11.3 Colombia MNIS and CENTRIXS Operations and Maintenance Support 115
5.2 On-Site, Off-Site, On-Call, Normal and Emergency Support 115
5.2.1 On-Site Support 115
5.2.2 Off-Site Support 115
5.2.3 On-Call Support 115
5.2.4 Performance of Services during National Crisis Declared by the President or Secretary of Defense 116
5.2.5 Performance of Services during Contingency, and Exercise Situations. 116
5.2.5.1 Remote Site Recovery 116
5.2.5.2 Failover Testing 116
5.2.5.3 Contingency and Emergency Planning. 117
5.2.5.4 Inclement Weather or other Natural or Manmade Disasters Emergency Services 117
5.2.5.5 Contingency and Exercise Supplemental IT Support Services 117
5.3 Special Requirements 117
5.3.1 Commercial Internet Service Provider (ISP) 117
5.3.2 TEMPEST Requirements 118
5.3.2.1 Provision or Use of IT 118
5.3.2.2 TEMPEST Accreditation 118
5.3.3 Invoice 118
5.4 Catastrophic Recovery and Support Acquisition Requirements 118
5.5 Contractor Response at Off-Site Locations 119
5.6 Meetings and Conferences 119
5.7 Contractor Manpower Reporting (CMR) 119
5.8 Reserved 120

5.9 Work Site 120
5.10 Changes to Operational Requirements 120
5.10.1. DoD Insourcing 120
5.10.2. Changes to Operational Requirements 121
PART 6 122
6. APPLICABLE PUBLICATIONS (CURRENT EDITIONS) 122
PART 7 127
PART 7 – ATTACHMENT 1 - TECHNICAL EXHIBIT 1 – Deliverable Requirements 129
(b)(3):10 U.S.C. § 130,(b)(7)(E) 157
(b)(3):10 U.S.C. § 130,(b)(7)(E) 159
(b)(3):10 U.S.C. § 130,(b)(7)(E) 162
(b)(3):10 U.S.C. § 130,(b)(7)(E) 165
(b)(3):10 U.S.C. § 130,(b)(7)(E) 167
PART 7 – ATTACHMENT 7 - TECHNICAL EXHIBIT 7 - Quality Assurance Surveillance Plan 169
ATTACHMENT 7 - APPENDIX 2: SAMPLE QUALITY ASSURANCE MONITORING FORM 182
ATTACHMENT 7 - APPENDIX 3 CUSTOMER COMPLAINT INVESTIGATON FORM 183
PART 7 – ATTACHMENT 8 - TECHNICAL EXHIBIT 8 - On-Site and On-Call Support Requirements 184
(b)(3):10 U.S.C. § 130,(b)(7)(E) 186
PART 7 – ATTACHMENT 10 - TECHNICAL EXHIBIT 10 - Maintained, Hosted, or Hoteled User Web Based or Command and Control Government Developed Applications 187
PART 7 – ATTACHMENT 11 – TECHNICAL EXHIBIT 11 – JIE Technical Implementation Guidelines 190
PART 7 – ATTACHMENT 12 - TECHNICAL EXHIBIT 12 - Reserved 191
PART 7 – ATTAHCMENT 13 - TECHNICAL EXHIBIT 13 – Functions Requiring Non-Disclosure Agreements 192
(b)(3):10 U.S.C. § 130,(b)(7)(E) 193
(b)(3):10 U.S.C. § 130,(b)(7)(E) 198
(b)(3):10 U.S.C. § 130,(b)(7)(E) 199

(b)(3):10 U.S.C. § 130,(b)(7)(E)

..... 201

PART 7 – ATTACHMENT 18 - TECHNICAL EXHIBIT 18 – Life Cycle Related Projects 202

PART 7 – ATTACHMENT 19 TECHNICAL EXHIBIT 19 – Level 1 and Level 2 Information Assurance Accreditation Package Work 203

PART 7 – ATTACHMENT 20 - TECHNICAL EXHIBIT 20 – Maintained Software Applications 210

PART 7 – ATTACHMENT 21 - TECHNICAL EXHIBIT 21 – Organizational Background Information 213

TCSC AOR/Functional Structure 222

Footprint 222

Additional Information 223

PART 7 - Attachment 22 - Technical Exhibit 22 – JTF-Bravo Unique Services 224

PART 7 - Attachment 23 - Technical Exhibit 23 – JTF-GTMO Unique Services 236

PART 7 - Attachment 24 - Technical Exhibit 24 – Software Engineering and Integration 246

PART 7 - Attachment 25 - Technical Exhibit 25 – Defense Cyber Operations and NetOps Tool Sets 247

PART 7 - Attachment 26 - Technical Exhibit 26 – Generic Network Diagram 248

PART 7 - Attachment 27 - Technical Exhibit 27 – Performance Requirements Summary 252

PART 8 - POINTS OF CONTACT 256

PART 9 - CONTRACT CLAUSES 257

PART 10 – Reports in ITSS and INVOICING 259

PERFORMANCE WORK STATEMENT (PWS)
FOR
U.S. SOUTHERN COMMAND (USSOUTHCOM)
ENTERPRISE INFORMATION TECHNOLOGY SERVICES SUPPORT CONTRACT (EITSSC)

PART 1
General Information

The scope of this Performance Work Statement (PWS) encompasses all aspects of the USSOUTHCOM (SC) Theater-wide Enterprise Information Technology Services Support Contract (EITSSC). The Contractor shall provide qualified, certified, and trained personnel, required items, and non-personal services necessary to perform the work required in this PWS. Work accomplished by the Contractor shall conform to the performance requirements outlined herein. Personnel assigned by the Contractor in support of tasks outlined in this effort may include a combination of on-site, off-site (at contractor or other Government facilities), and on-call program managers, project managers, information technology life cycle support advisors, engineers, technicians, system administrators, and software developers, as well as, communications systems support specialists such as trainers, logisticians, configuration managers, and transportation specialists. These personnel shall operate and maintain, upgrade, modernize, reconfigure, or provide support services related to SC information technology (IT) / information management (IM) systems and communications system (CS) and associated networks identified in this PW, as well as, future envisioned or planned systems. For simplification, the term information technology (IT) shall include information technology systems or components, communications systems or components, information management systems, or software applications.

Currently, the SC Theater consists of the following independent IT environments sustained under independent contracts or managed by Government personnel.

- SC HQ – 525th Signal Company IT Support Contract– Approx. 2500 Users
- Theater C4 Support Center (TCSC) – Security Cooperation Offices – Approx. 1000 Users, and Multinational Information Sharing Systems (MNIS) – Approx. – 400 Users
- Joint Task Force Guantanamo Bay, (JTF-GTMO) Cuba – Approx. 1000 Users
- Joint Task Force Bravo, (JTF-Bravo) Honduras – Approx. 800 Users

The locations and associated contracts for these environments, plus other service requirements consolidated under this requirement, are identified in Attachment 3; these IT environments and associated IT support requirements shall all transfer to this single EITSSC contract. Attachments 2 and 21 contain historical information related to the past IT support contracts for the 525th Signal Company, JTF-Bravo, JTF-GTMO, and TCSC. Through the Joint Information Environment (JIE) transformation efforts identified in this Task Order, the SIPRNET, NIPRNET, and Internet environments at all locations shall transition to common information environments within their respective security domains. In other words, there shall no longer be different

Secure Internet Protocol Router Network (SIPRNET), Nonsecure Internet Protocol (IP) Router Network (NIPRNET), and Internet environments at each of the above locations.

1. GENERAL

This is a non-personnel services contract to provide IT life cycle support, IT modification, new IT systems integration, and IT systems support services. The Government will not exercise supervision or control over Contractor service provider personnel performing the services herein. The Contractor shall hold contract service providers accountable for all aspects of this Task Order; the Contractor, in turn, is responsible to the Government.

1.1 Description of Services/Introduction

Unless otherwise specified, the Contractor shall provide personnel, equipment, supplies, facilities, transportation, tools, materials, supervision, and other items and non-personal services necessary to develop, implement, operate and maintain, and support IT except for those items specified as government furnished property/government service equipment and services. The term Government Furnished Equipment or GFE, applies to equipment, facilities, or other required services. The Government reserves the right to provide equipment, facilities and other required services as government furnished equipment, facilities or services on this Task Order; the Contractor shall integrate and assume responsibility for any GFE. The Contractor shall perform to the standards in this Task Order.

There are 9 major types of IT services to be provided in this effort; the first 5 are adapted within the construct of the DoD Enterprise Service Management Framework (DESMF) and Army Information Technology Service Management (ITSM) Policy. The 9 major types of services are found in Section 5.1.

1.2 Background

SOUTHCOM J6 (SCJ6) is tasked by the Combatant Commander to implement and sustain U.S. and multinational IT to support full spectrum operations in the SC Area of Responsibility (AOR) which is currently Central America, South America, and select countries in the Caribbean. Currently, this is accomplished through the execution of multiple contracts aligned to specific operating locations or communities of interests. Under this effort, the Contractor shall assume responsibility for the IT services and associated contracts identified in Attachment 3. Attachment 4 contains a list of IT infrastructure, systems, and components that the Contractor shall support through their life cycle; this list is developed in accordance with Army Regulation 25-1, Army Information Technology, Appendix B and identifies all system registered in the Army Portfolio Management Solution (APMS). Other systems to be registered in APMS are also included.

In accordance with DoD CIO guidance to migrate to a single JIE, as well as, future 20 percent reduction in headquarters resources, SC will no longer sustain independent contract/Task Order efforts for provisioning and lifecycle sustainment of NIPRNET, SIPRNET, certain unclassified MNIS systems, and in the case of JTF-GTMO, Joint Worldwide Intelligence Communications System (JWICS) services.

1.3 Objectives

The objective of this Task Order is to establish a program of support for SC HQ, Security Cooperation Offices (SCOs), Direct Reporting Units (DRUs), and MNIS communities of interest that provides secure, seamless, effective, and efficient enterprise IT support. In addition to providing IT life cycle support efforts across the Area of Responsibility (AOR), the Contractor shall prepare, integrate, and transition all networks to JIE standards, as well as, make the networks compatible with Unified Capabilities (UC) requirements which include:

- Transitioning to a Single Security Architecture (SSA) with common security capabilities and processes to include remote management of all information assurance devices from the SC HQ facility.

- Standardize methods to authenticate and access data and data processing resources through implementation of a single architecture for Identity and Access Management (IdAM) managed from the SC HQ facility.

- Normalization of all Active Directory structures across the Networks in accordance with network normalization requirements, as well as, to include migration to a single set of Active Directory per domain class (SIPRNET, NIPRNET, Internet, etc.) to include remote management of all Active Directories from the SC HQ facility.

- Ensuring software application rationalization and server virtualization in accordance with DoD Data Center Consolidation guidelines. This includes eliminating duplicate functional equivalents and ensuring common access to these systems across the AOR, as well as, migrating appropriate applications to DoD or SC Enterprise Services.

- Migrating appropriate traditional server and client based applications to a Software-as-a-Service model and if beneficial, cloud computing. This entails migrating appropriate client and server based applications to Hosted Services (Cloud Computing) either at the SC HQ facility, a Defense Information Systems Agency (DISA) Defense Enterprise Computing Center (DECC), or to an DoD approved Commercial Cloud Service Provider.

- Remotely managing and consolidate data centers and all associated IT infrastructure to the maximum extent possible given the available resources.

- Deprecating (merging with the SC HQ) and normalizing independent network enclaves while

modernizing voice, data, and video technologies. This includes replacing appropriate voice, data, and video components with those on the DISA approved UC list.

- Studying and implementing an approved client modernization architecture.

- Integrating all independent Mobility Services.

In addition, the Contractor shall streamline similar functions across all organizations to include:

- Implementing a single Service Desk function operating from the HQ USSOUTHCOM facility

- Standardizing and migrating to a single platform, all Service Desk applications to include incident reporting systems, service request systems, and property accountability systems.

- Standardizing and moving to common processes and tools, support functions such as configuration management, logistics, and procurement.

Finally, the contractor shall support the integration of new capabilities across the AOR. Note that the Government reserves the right to implement any new capability through other means and provide the solutions as GFE to the Contractor for continued life cycle support just as all the current systems are considered GFE.

1.4 Scope

The efforts supported under this performance work statement are specifically related to information technology life cycle support required across the SC AOR. This includes ancillary tasks identified as critical to basic IT support or IT use at specific locations.

1.5 Period of Performance

The period of performance shall be for one (1) Base Period of 12 months and six (6) 12-month option periods. The Period of Performance reads as follows:

- Base Period (1 Year)
- Option Period 1
- Option Period 2
- Option Period 3
- Option Period 4
- Option Period 5
- Option Period 6

1.6 General Information

1.6.1 IT Life Cycle Execution and Quality Control

The Contractor shall support all life cycle aspects of IT development, operations, maintenance and use. The Contractor shall develop and execute processes and procedures in accordance with commercial and government best practices for IT life cycle activities and adapted as required to meet the requirements of this PWS. Concurrently, the Contractor shall develop and implement quality control procedures to identify, prevent, and ensure non-recurrence of defective services. The Contractor's quality control program is the means by which they assure their work complies with the requirement of this Task Order. Performance on this Task Order shall be measured against the Performance Requirements Summary in Attachment 27 using the Quality Assurance Surveillance Plan as described in Attachment 7. See paragraph 5.1 for more details.

(Deliverable # 3, Attachment 1)

1.6.2 Quality Assurance

The Government will evaluate the Contractor's performance under this Task Order in accordance with the Quality Assurance Surveillance Plan (See Attachment # 7).

1.6.3 Recognized Holidays

In general, the Contractor shall follow the holiday schedule below, but may be required to perform services on these days based on specific PWS requirements. The following are the recognized holidays for this effort.

- New Year's Day
- Martin Luther King Jr.'s Birthday
- President's Day
- Memorial Day
- Independence Day
- Labor Day
- Veteran's Day
- Columbus Day
- Thanksgiving Day
- Christmas Day

Foreign Nationals working in Colombia and Honduras shall observe mandatory holidays for their respective countries. The Contractor shall identify those days after completion of appropriate subcontracts or hiring actions in Colombia and Honduras are in place.

1.6.4 Hours of Operation

The Contractor shall at all times maintain an adequate workforce for the uninterrupted performance of all tasks defined within this PWS. When addressing internal personnel transfers or hiring personnel, the Contractor shall keep in mind the stability and continuity of the workforce are essential.

The following hours of operation apply.

a. Tier 1, 2, and 3 Services. The Contractor shall provide Tier 1, Tier 2, and Tier 3 services during normal local duty hours (0600 to 1800, Monday through Friday) at SC HQ, JTF-Bravo, and JTF-GTMO. These hours may be covered on a staggered shift schedule. Note that JTF-GTMO and JTF-Bravo have additional coverage requirements; see attachments 22 and 23.

b. Incident Reponses. During normal duty hours, the Contractor shall provide incident problem identification and response times within 15 minutes at SC HQ, Joint Task Forces and Security Cooperation Offices (SCOs) with permanent personnel. After hours and on holidays, the Contractor shall provide a two-hour response time to IT related incidents or concerns at SC HQ and Joint Task Forces and SCOs with permanent personnel. For SCOs without permanent on-site support, the Contractor shall provide twenty-four hour response time, country clearance process permitting.

c. Service Desk Services. Once integrated across the Theater, the Contractor shall support the integrated Service Desk shall from 0500 to 2000 EST Monday through Friday. The Contractor shall provide a separately priced option to operate the Service Desk 24 hours per day, 7 days a week; additional Contractor personnel shall only reside at USSOUTHCOM HQ. The 0500 – 2000 Service Desk Services window may shift based on operational needs.

d. Theater Network Coordination Center (TNCC) and Technical Control Facility (TCF) Services. The Contractor shall provide TNCC and TCF services at SC HQ 24 hours per day, 7 days a week.

e. Conference Room Services. The Contractor shall provide Conference Room support services from 0600-1900 Monday- Friday local time at SCHQ, JTF-Bravo, JTF-GTMO and Bogota, Colombia. The 0600 – 1900 Conference Room Services window may shift based on operational needs.

f. Video Teleconferencing (VTC) Services. The Contractor shall provide VTC support services from 0600-1900 local time throughout the AOR. The 0600 – 1900 VTC Support window may shift based on operational needs.

1.6.5 Place of Performance

The Contractor shall perform on-site, off-site, and on-call work under this Task Order at the locations identified in Attachment 8. Temporary or permanent work may be added to any CONUS or OCONUS locations in the SC AOR by the Changes Clause and subsequent contract modification.

1.6.6 Type of Contract

This Task Order is a hybrid Firm Fixed Price, Time and Materials, and Per Diem/Cost Reimbursement for Travel and Overseas Housing. Refer to the Price Schedule for contract type information, by CLIN.

1.6.6.1 Additional Hours greater than 40 Hours Per Week.

Contractor expenditure of hours above 40 per week for any position requires coordination with the COR. The Contractor shall receive the approval of the COR prior to working additional hours during regular duties, contingency operations or exercise support. Additional hours are defined as work accomplished in addition to normal hours programmed on any specific position on a monthly basis.

1.6.7 Security Requirements

Contractor personnel performing work under this Task Order shall maintain security clearances appropriate with their responsibilities before they can start work on this effort. Contractor personnel shall also maintain appropriate security clearances for the duration of their support on this Task Order. Interim clearances at appropriate security levels for respective positions, is authorized. (See paragraph # 4.2 or more details.)

1.6.7.1 Physical Security

The Contractor shall safeguard all government equipment, information and property provided for Contractor use; the Life Cycle Implementation and Quality Control Plan (LCIQCP) shall address the methods for safeguarding equipment, information and property. The Contractor shall secure government facilities, equipment, and materials at the close of each work period. When solely responsible for a Government provided workspace, the Contractor shall use Standard Form 701 and 702 physical security logs. When sharing a space with the Government, the Contractor shall share responsibilities for maintaining the Standard Form 701 and 702 physical security logs. (Deliverable # 3 Attachment 1)

1.6.7.2 Key Control

The Contractor shall establish and implement procedures for controlling keys/key cards issued to the Contractor by the Government; the LCIQCP shall address the procedures for controlling keys and key cards. Such procedures shall include turn-in of any issued keys/key cards by

personnel who no longer require access to locked areas. The Contractor shall not duplicate keys/key cards issued by the Government. The Contractor shall immediately report any occurrences of lost or duplicate keys/key cards to the COR. (Deliverable # 3 Attachment 1)

1.6.7.2.1 Lost Keys

In the event keys, other than master keys, are lost or duplicated, the Contractor shall, upon direction of the Contracting Officer, re-key or replace the affected lock or locks; however, the Government, at its option, may replace the affected lock or locks or perform re-keying. When the replacement of locks or re-keying is performed by the Government, the total cost of re-keying or the replacement of the lock or locks will be deducted from the next periodic payment due the Contractor. In the event a master key is lost or duplicated, all locks and keys for that system will be replaced by the Government and the total cost deducted from the next payment due the Contractor.

1.6.7.2.2 Use of Keys by Other Persons

The Contractor shall prohibit the use of Government-issued keys/key cards by any persons other than the personnel working on this effort. The Contractor shall prohibit the opening of locked areas to permit entrance of persons other than personnel engaged in the performance of assigned work in those areas, or personnel authorized entrance by the COR.

1.6.7.3 Lock Combinations

The Contractor shall establish and implement procedures to ensure lock combinations are not revealed to unauthorized persons. The Contractor shall ensure that lock combinations are changed when personnel having access to the combinations no longer have a need to know such combinations. The Contractor shall include these procedures in the LCIQCP. (Deliverable # 3 Attachment 1)

1.6.7.4 Reporting Security Incidents

The Contractor shall report and start investigations of all physical and network security violations within 24-hours of the incident to the COR. The Contractor shall initiate protective/corrective measures when a security incident or vulnerability is discovered. The Contractor shall address the process for reporting security incidents in the LCIQCP (Deliverable # 3, 42, Attachment 1).

1.6.8 Special Qualifications

1.6.8.1 Qualified Contractor Support Personnel

The Contractor shall maintain an adequate work force with the proper certifications for the uninterrupted performance of all tasks defined within this performance work statement. When hiring personnel, the Contractor shall keep in mind that the stability and continuity of the work force are essential. As a sub-plan to the LCIQCP, the Contractor shall develop and maintain a retention plan to retain IT subject-matter-experts on hand (Deliverable # 3 Attachment 1).

1.6.8.2 Personnel Resumes

The Contractor shall have the personnel, organization, and administrative control necessary to ensure that the services performed meet all requirements specified in this Task Order. The Contractor shall provide personnel with appropriate experience directly related to the tasks and functions to be assigned. The COR reserves the right to determine if a given work history contains necessary and sufficiently detailed, related experience to reasonably ensure the ability for effective and efficient performance. The COR may request to review resumes of Contractor personnel being considered to perform or currently performing the requirements of this PWS. If the COR questions the qualifications or competence of any person performing under the contract, the Contractor shall sustain the burden of proof to demonstrate the person's qualifications. The Contractor shall present to the COR, for their approval, the resumes of personnel relocating to JTF-Bravo, JTF-GTMO and any Security Cooperation Office prior to the Contractor's initiation of country clearance requests. The Contractor shall receive approval prior to proceeding with relocation of personnel to JTF-Bravo, JTF-GTMO, or the Security Cooperation Offices. Resumes of Key Personnel will be made available at any time.

1.6.8.3 Computing Environment, Technical, and Functional Area Training of Contractor Personnel

The Contractor shall provide personnel with the required core skills and experience to perform their job duties. The Contractor shall provide training to build or maintain expertise of contractor personnel assigned to this Task Order at its own expense except when the Government has given prior approval for training to meet special requirements that are peculiar to a particular task. Training of Contractor personnel will not be reimbursed when the Government mandates changes to Information Technology/Information Management (IT/IM) software (user applications, platform applications, or infrastructure support applications) as a result of Life Cycle updates or end-of-life replacements during the performance of ongoing tasks. Given that all IT environments change every 24 to 60 months, the Contractor shall ensure computing environment certification and training of personnel as part of Life Cycle modernization processes. Contractor personnel shall attend seminars, symposiums, or user group conferences only if the Government certifies that attendance is mandatory for the performance of the task requirements and the COR approves such training in advance. Reimbursement for computing environment training shall not be authorized for replacement contractor personnel; for the purpose of keeping contractor personnel abreast of advances in the state of the art; nor for training contractor personnel on equipment, computer languages, or computer operating systems that are available on the commercial market.

The Contractor shall address in the LCIQCP how personnel supporting this Task Order shall attain and maintain the appropriate computing environment certifications and training to plan, design, transition, operate and maintain all systems found on USSOUTHCOM IT environments. The Contractor shall track required training and certifications on a by-system and by-personnel basis. Required certifications and training shall be accomplished within 3 months of assuming responsibility for any location or system (Deliverables #3, 99 Attachment 1).

The Contractor shall also address how they shall keep contractor personnel trained and abreast of advances in standard commercial and government-developed technologies in the LCIQCP. In addition to the core competencies related to their jobs, The Contractor shall ensure that the personnel are trained on customer support protocols and customer relations. The Contractor shall ensure that their personnel are trained on the protocols associated with the support of all ranks of the military, civilian, contractor, and interagency members of a Joint Command.

All Contractor personnel supporting Software Engineering and Integration shall have hands-on experience in modeling, developing, integrating, and/or deploying applications in accordance with the Software Engineering and Integration (SEI) Policy.

Contractor Personnel supporting Database Administration shall have hands-on experience and certifications in developing, deploying, and maintaining SQL and MySQL databases and in the case of GCCS, Oracle databases commensurate with the systems supported in this PWS.

Contractor personnel supporting System Administration shall have hands-on experience and certifications in developing, deploying, and maintaining Windows, LINUX, and UNIX operating systems with the systems supported in this PWS. The Contractor personnel supporting System Administration shall also have OEM certifications for all operated and maintained systems upon assumption of responsibilities for existing systems or prior to transition to operations any new or modified system.

Contractor personnel supporting networking shall have hands-on experience designing, configuring, deploying and troubleshooting to include, but not limited to, Cisco, Netscout, Infoblox, Gigamon RSA, Juniper, VMware, Splunk and Websense technologies. Adequate Contractor personnel in these functions shall be certified as Cisco Certified Internetwork Expert (CCIE), Cisco Certified Network Professional (CCNP), and Certified Network Professional in Routing/Switching, Security, and Data Center with appropriate levels of experience commensurate with the systems supported in this PWS.

Contractor personnel supporting the Audio/Video/Voice Systems shall have hands-on experience designing, configuring, deploying and troubleshooting to include, but not limited to, Cisco, Vbrick, AMX, Polycom, Barco, as well as Public Address Systems and other audio/visual reinforcement and rebroadcast equipment. Adequate Contractor personnel in these functions shall have Cisco Certified Network Associates (CCNA), Cisco Certified Network Professionals

(CCNP), and Cisco Certified Internetwork Experts (CCIE), certifications appropriate levels of experience commensurate with the systems supported in this PWS.

Contractor personnel supporting TEMPEST equipment must be certified on TEMPEST equipment on a by-equipment basis.
(Deliverable # 3 Attachment 1)

1.6.8.4 Information Assurance Certification of Contractor Personnel

The Contractor shall train personnel filling positions requiring DOD mandated Information Assurance certifications at the expense of the Contractor unless the certification requirement was established after award of this Task Order. The Contractor shall ensure the certification compliance in accordance with (IAW) DoD 8570.01-M Information Assurance Workforce Improvement Program. The Contractor shall ensure that all contractor personnel shall have certifications for their specific computing environment commensurate with their responsibilities and labor categories prior to the start of work on this Task Order.

The Contractor shall ensure that all TIER I/TIER II support personnel obtain and maintain certification corresponding to Information Assurance Technical Level I (IAT I).

Personnel performing functions as Application Support are required to obtain and maintain certification corresponding to Information Assurance Technical Level II (IAT II).

Personnel performing functions as Systems Administrators or Enterprise System Administrators are required to obtain and maintain certification corresponding to Information Assurance Technical Level II (IAT II).

Personnel performing functions as Network Technicians are required to obtain and maintain certification corresponding to Information Assurance Technical Level III (IAT III).

Personnel performing functions as Engineers are required to obtain and maintain certification corresponding to Information Assurance Technical Level III (IAT III).

Personnel performing functions as Network Security Technicians are required to obtain and maintain certification corresponding to Information Assurance Technical Level III (IAT III).

The Contractor shall ensure all personnel meet the minimum certification requirements within six months of the task order award. Further, The Contractor shall ensure all new hires meet the minimum requirements for their respective positions upon initiation of their duties. Contractor Technical Level I, II and III personnel shall also obtain the appropriate computing environment certification/s required by their employing organization (DOD 8570.01-M, para. C3.2.4.8.3). The Contractor shall be responsible for yearly maintenance fees to keep these certifications. This includes but is not limited to 120 Continuing Professional Education credits (CPEs) every three

years. The Contractor shall provide a list on a by position basis of the required training and status of certifications in the LCIQCP (Deliverable #3 Attachment 1).

Contractor personnel performing engineering, system administration, or network manager functions with privileged-level access to control, manage, or configure Government information systems shall meet training and certification requirements for Information Assurance (IA) Support Personnel as specified DOD 8570.1. Admission to this training requires satisfactory completion of both the Information Assurance Security Officer (IASO) Management Level I and Information Assurance Technical Level I courses. Contractor personnel shall complete refresher training every 18 months.

Contractor personnel performing Communications Security (COMSEC) support shall demonstrate:

- Three (3) years of experience in telecommunications circuit/network encryption requirements to include in-depth knowledge of Controlled Cryptographic Items (CCI) equipment, operation, and associated keying material (traditional and electronic). Background must cover both the tactical and strategic telecommunications encryption infrastructure.

- Three (3) years of experience in National Security Agency (NSA) COMSEC account custodian or custodian of a DoD Service Local COMSEC Management Software (LCMS) Electronic Key Management System (EKMS) account.

- Three (3) years of experience with the NSA Distributed Information Security (INFOSEC) Accounting System (DIAS) and National Security Agency/Central Security Service (NSA/CSS) Policy Manual 3-16 on Control of COMSEC Material.

- Three (3) years of experience the National Industrial Security Program Operating Manual (NISPOM) and related DoD requirements for protecting classified information including requirements pertaining to the general safeguarding, control, transmission, disposition and retention of classified material. The Contractor personnel shall possess a minimum of three (3) years of experience on security classification and classification markings, to include knowledge of physical security requirements for secure rooms and vaults and will possess the knowledge and ability to inspect proposed/existing COMSEC facilities for compliance.

- COMSEC personnel shall also maintain technical knowledge base and keep current in all aspects of emerging technologies associated with or impacting on KMI, including all new crypto modernization equipment/products such as the High Assurance Internet Protocol Encryptor(s) (HAIPE); and new Secure Communication Interoperable Protocol (SCIP) devices such as the OMNI (an encryption device by this name); Sectera Wireline Terminal (a type of telephone encryption device), Secure Telephone Equipment (STE) and GSM (a type of secure telephone instrument).

Contractor personnel supporting Level 1 and 2 Cyber Security functions shall attain IAT and IAM certifications in accordance with DoD 8570-01-M appropriate to the functions being accomplished (Deliverable 3 and 99, Attachment 1).

1.6.8.5 Driver Qualifications

The Contractor shall ensure that personnel which operate government-owned vehicles have a valid driver's license, and have completed the vehicle driving accident avoidance course. Contractor is responsible for having a valid insurance policy to protect personnel and vehicle.

1.6.8.6 DoD/USSOUTHCOM Required Training

All Contractor personnel shall demonstrate current certificates (within 1 year) or take the following required on-line or in-class training upon commencement of work on this contact; the Contractor shall address the method for compliance in the LCIQCP. (Deliverable #'s 3, 75, Attachment 1)

- Local LAN User Course
- Cyber Awareness Training
- Level 1 Anti-Terrorism Awareness Training
- Identifying and Safeguarding Personal Identifiable Information
- Combatting Trafficking in Persons in the SOUTHCOM AOR
- Destructive Weather and Hurricane Preparedness
- Operations Security (OPSEC) Refresher
- Annual Security Awareness
- Operations Security (OPSEC) Level 1
- ISOPREP and SERE 100.1 Level A Training For those Traveling OCONUS
- Emergency Response and Active Shooter Preparedness
- Sexual Harassment Assault Response (SHARP)
-)

1.6.8.6.1 Training on Combatting Trafficking in Persons

In accordance with FAR 52.222-50, The Contractor shall notify its personnel of:

a. The United States Government's zero tolerance policy described in paragraph (b) of this clause.

b. Actions the Contractor shall take against personnel for violations of this policy. Such actions may include, but are not limited to, removal from the contract, reduction in benefits, termination of employment, and reporting to appropriate law enforcement officials.

All contractor personnel on this Task Order shall take appropriate DoD approved on-line training and demonstrate certificates of completion on a yearly basis. The Contractor shall post certificates on the SC Training Portal, as well as, maintain as records.
(Deliverable # 75, Attachment 1)

1.6.9 Post Award Conference/Quarterly Progress Review Meetings

The Contractor shall support a post award conference, as well as, Quad Monthly progress review meetings convened by the contracting activity or contract administration office in accordance with Federal Acquisition Regulation Subpart 42.5. The Contractor shall support a Post Award Conference 2 Weeks after start of first period of performance. The Contractor shall submit Monthly Progress Briefings and support an associated Monthly Progress meeting throughout the first four months of the start of the first period of performance. After this time, the Contractor shall support Quad-Monthly Progress meetings throughout the balance of the task order. A determination to move to bi-annual Progress Reviews will be made as part of the subsequent options.

Additionally, the Contractor shall meet, as appropriate, with the COR, Regional and Functional ACORs, and other Government personnel, to review the Contractor's performance. At these meetings the contracting officer will apprise the Contractor of how the government views the Contractor's performance and the Contractor shall apprise the Government of problems, if any, being experienced. The Contractor shall take appropriate action to resolve outstanding issues. The Contractor shall ensure that the Regional ACORs and functional ACORs are notified of any technical degradations, outages, or changes, as soon as possible. The Contractor shall also notify ACORs, and Functional ACORs of any planned or possible future changes tasked by the COR.Contractor participation in these meetings is included in the cost of the contract stated elsewhere and shall be at no additional cost to the Government. The Contractor shall submit minutes of all items discussed and any action items. (Deliverable # 1 Attachment 1)

1.6.9.1 Periodic Progress, Status, and Management Report

The Contractor shall submit periodic reports to the COR, as well as, Regional, and Functional ACORS outlining the status of the program to include: Major activities or modifications accomplished, labor hours expended, upcoming major activities or modifications, personnel changes, and summary of travel accomplished. (Deliverable # 2 Attachment 1)

1.6.10 Contracting Officer Representative (COR)

The COR will be identified by separate letter. The COR is responsible to the Contracting Officer to monitor all aspects of the contract and assists in contract administration. The COR is authorized to perform the following functions:

a. Ensure that The Contractor performs the requirements of the contract.

b. Ensure accomplishment of inspections as necessary in connection with contract performance.
c. Maintain written and oral communications with the Contractor concerning technical aspects of the contract.
d. Ensure accomplishment of written interpretations of technical requirements, including Government drawings, designs, and specifications
e. Ensure monitoring of Contractor's performance notifies both the Contracting Officer and Contractor of any deficiencies.
f. Coordinate availability of government furnished property/information, and provide site entry of Contractor personnel.

A letter of designation issued to the COR, a copy of which is sent to the Contractor, states the responsibilities and limitations of the COR, especially with regard to changes in cost or price, estimates or changes in delivery dates, and the delegations of that letter supersede any inconsistencies with this paragraph. The COR is not authorized to change any of the terms and conditions of the resulting order. A COR appointment letter will be provided upon award.

1.6.10.1 Assistant Contracting Officer Representatives (ACORs)

Due to the diversity of services on this Task Order, the Government will assign multiple ACORs supporting the requirements of SC HQ, JTF- Bravo, and JTF-GTMO or program technical/functional areas. The ACOR titles are identified below. ACORs monitor technical and functional aspects of the contract on a theater-wide basis, as well as, administrative aspects of the contract on a regional basis.

A letter of designation will be issued to each ACOR, a copy of which will be sent to the Contractor. ACORs are not authorized to change any of the terms and conditions of the resulting order.

1.6.10.1.1 ACORs by Regional or Functional Area

a. USSOUTHCOM IT Service Operations (Includes SCOs and SOUTHCOM Washington Field Office (SCWFO)
b. JTF-Bravo IT Service Operations
c. JTF-GTMO IT Service Operations
d. User Support Services (GCCS, MNIS, SharePoint, Training)
e. Enterprise Service Strategy, Design, and Transition
f. Continual Service Improvement
g. Enterprise Support Services (Logistics, Procurement)
h. Cyber Security (Information Assurance) Level 1
i. Enterprise Configuration Management (Excluding Policy)
j. Enterprise Software Engineering and Integration
k. JTF-GTMO Unique Services (JDIMS, JWICS, and Physical Security)

l. Enterprise Data Networks Capabilities
m. Enterprise Data Storage Capabilities
n. Enterprise Data Processing Capabilities
o. Enterprise Audio/Video, VTC and Voice Capabilities
p. Enterprise Technical Control, Data Center, Cable Plant, LMR, Microwave and SATCOM

1.6.11 Contractor Key Personnel

The Contractor shall assign and identify the following key personnel to provide management, administrative, and technical interaction with Government members in the day-to-day accomplishment of support services. The Contractor shall submit the qualifications of each employee for Government review prior to placing individuals into the key personnel positions identified below. The Contractor may designate and identify additional contractor personnel considered key to operations for efforts under this task order. These key personnel shall have an in-depth understanding of the requirements and their responsibilities as well as the ability, knowledge, experience, and skills to perform the requirements. The Contractor shall maintain the names of the key personnel in the LCIQCP. The Contractor may assign a given individual as lead to more than one function for areas “k” through “s”.

a. Program/Contract Manager
b. Enterprise Quality Assurance/Continual Service Improvement Lead
c. Deputy Program Manager for USSOUTHCOM HQ and SCO Service Operations
d. Deputy Program Manager for JTF-Bravo Service Operations
e. Deputy Program Manager for JTF-GTMO Service Operations
f. Enterprise User Support Services (GCCS, MNIS, SharePoint, Training)
g. Enterprise IT Systems Support Services (Logistics, Procurement) Lead
h. Enterprise Configuration Management Lead
i. Enterprise Cyber Security and Information Assurance Level 1 Lead
j. Enterprise Software Engineering and Integration/Application Development and Operations Lead
k. Enterprise Service Strategy Lead
l. Enterprise Service Design Lead
m. Enterprise Service Transition Lead
n. Enterprise Data Networks Capabilities Lead
o. Enterprise Data Storage Capabilities Lead
p. Enterprise Data Processing Capabilities Lead
q. Enterprise Audio/Video, VTC and Voice Capabilities Lead
r. Enterprise Tech Control, Data Center, Cable Plant, LMR, Microwave and SATCOM Lead

(Deliverable # 3 Attachment 1)

1.6.12 Identification of Contractor Personnel

All contract personnel attending meetings, answering Government telephones, and working in other situations where their contractor status is not obvious to third parties are required to identify themselves as such to avoid creating an impression in the minds of government personnel, other contractors, or members of the public that they are Government officials. Such confusion can result in the improper release of information to or by these individuals. Contractor shall also ensure that all documents or reports produced by contractors are suitably marked as contractor products or that contractor participation is appropriately disclosed. Contractor personnel shall obtain and wear Government-issued Common Access Card (CAC) and/or Government facility badges provided at assigned posts.

1.6.13 Contractor Travel Expense Reimbursement

Contractor personnel shall be required to travel in CONUS (any state in USA), within the NCR and OCONUS (any country in Central, South America, and the Caribbean) or on occasion to other Theaters of Operation to accomplish the tasks contained in this PWS to include performing work, attending meetings, conferences, and training. The Contractor may be required to travel to off-site training locations and to ship training aids to these locations in support of this PWS.

The Contractor shall be authorized travel expenses for all efforts except those in paragraph 1.6.9, consistent with the substantive provisions of the Joint Travel Regulation (JTR) and the limitation of funds specified in this Task Order. All travel except for that identified in paragraph 1.6.9 requires Government approval/authorization and notification to the COR. The Contractor shall forecast travel on a quarterly basis for all efforts in this Task Order and submit those requirements for approval to the COR.

Costs for transportation may be based upon mileage rates, actual costs incurred, or a combination thereof, provided the method used results in a reasonable charge. Travel costs shall be considered reasonable and allowable only to the extent that they do not exceed on a daily basis, the maximum per diem rates in effect at the time of the travel. The Joint Travel Regulations (JTR), while not wholly applicable to contractors, shall provide the basis for the determination as to reasonable and allowable. Maximum use is to be made of the lowest available customary standard coach or equivalent airfare accommodations available during normal business hours. The Contractor shall request approval from the COR for all necessary travel meeting the above criteria.

(Deliverable # 3, 4, 5, Attachment 1)

1.6.13.1 Theater and Country Clearances

All Contractor personnel traveling to OCONUS locations shall have approved theater and country clearances. This includes obtaining VISAs and satisfying any and all OCONUS location requirements (if any), to include without limitation Status of Forces Agreements (SOFA) and/or

Technical Expert Status Accreditation (TESA) requirements as and when required, prior to travel. All contractor personnel shall coordinate appropriate theater and country clearance approvals with the COR. The Contractor shall forward theater and country clearance requests to SC at least 30 days prior to the date of travel. SC will approve all theater clearance requests; and the Department of State (DoS) will approve all country clearance requests. The Contractor shall not travel to OCONUS locations without having approved theater and country clearances. Additionally, the COR will issue Invitational Travel Orders (ITOs) to contractor personnel who are required to travel. The government will not process theater and country clearance requests without the mandatory training. Exceptions to the above policy will be made on an as-needed-basis for major system or capability outages by the COR; the COR may give email based approval under these circumstances. The Contractor shall accomplish close coordination with the COR and the appropriate ACOR. The Contractor shall identify the process for implementing Theater and County Clearances in the LCIQCP. (Deliverable # 2, 3, 6, 7 Attachment 1)

1.6.13.2 OCONUS Travel Security and Other Related Requirements

The Contractor shall travel to the locations approved by the COR. All Contractors shall adhere to the Force Protection rules mandated by the Regional Security Officer (RSO) and the Security Cooperation Office (SCO) Commander. Prior to travel from CONUS, all Contractor personnel shall accomplish mandatory pre-travel, Force Protection (Anti-Terrorist/Force Protection Level I) training; Human Rights training, and Personnel Recovery training. Force Protection and Human Rights training are unclassified and personnel shall obtain at least an 80 percent score on the Human Rights training test. Personnel Recovery training consists of six unclassified and one classified video. At the conclusion of Personnel Recovery training, the Contractor shall ensure all personnel that travel complete an Isolated Personnel Report (ISOPREP), and file the ISOPREP with the appropriate SC organization and the ACOR prior to travel. In addition to the pre-travel training requirements, personnel traveling to areas considered to be hostile within designated OCONUS locations are required to take additional training as mandated by the RSO and SCO Commander. The Contractor shall address the process for OCONUS Travel Security in the LCIQCP.

The Contractor shall also certify that OCONUS travel on official business related to this Task Order is reported to the Defense Security Service if required.

In addition, the Contractor shall keep track and submit yearly reports of all OCONUS travel to include the list of personnel, locations traveled, purpose, and training accomplished.

(Deliverable # 3, 8 Attachment 1)

1.6.13.2.1 ISOPREP Requirements Details.

Prior to deploying to any country, US contractor personnel shall meet the USSOUTHCOM requirements for Force Protection Training and comply with the requirements for the Isolated

Personnel Report (ISOPREP), DD Form 1833. Once completed, the ISOPREP becomes a document classified as Confidential. Because of the security classification, the ISOPREP must be completed on a classified computer system, or the DD Form 1833 can be downloaded, printed out, completed by hand (legibly), and then the classified document mailed (in accordance with DOD policy) to HQ, USSOUTHCOM J3 Directorate, 9301 NW 33rd Street, Doral, FL 33172-1217. All personnel deploying to any country shall coordinate the submission of the appropriate theater and host nation country clearance approvals with the COR and USSOUTHCOM S&I. The Contractor shall comply with AR 380-19 paragraph 2-16 (U.S. personnel) and AR 380-19 paragraph 2-17 (Local National) prior to employment.

1.6.14 Other Direct Costs

The following services and items shall be treated as Other Direct Costs (ODCs)

a. Travel
b. Overseas Housing Allowance
c. Personnel Relocation
d. Equipment Procurements (Spares, Life Cycle, or any New Capability)
e. Warranties for any equipment
f. Software Licenses
g. Shipping Costs
h. Satellite or Internet Service Costs
i. Import or Export Tariffs or Fees
~~j. Foreign National labor~~
k. War Risk Insurance
l. DBA Insurance
m. Medical/Dental insurance for personnel at GTMO
n. COLA
o. Post Hardship Differential
p. Danger Pay

1.6.15 Data Rights

The Government has unlimited rights to all documents/material produced under this Task Order. By accepting this task order the Contractor acknowledges that all documents and materials, to include the source codes of any software, and any process/business processes developed or produced under this Task Order shall be Government owned and are the property of the Government with all rights and privileges of ownership/copyright belonging exclusively to the Government. The Contractor may not use or sell these documents and materials without written permission from the Contracting Officer. All materials supplied to the Government will be the sole property of the Government and may not be used for any other purpose. This right does not abrogate any other Government rights. The Government intends to use in information generated on this Task Order to include all deliverables, on future Government requirements.

Reference DFAR clause (252.227-7014) Rights in Non-commercial Computer software and noncommercial computer software documentation.

1.6.16 Organizational Conflict of Interest

Contractor will be tasked to provide Consultants and OEM support or to procure OEM Hardware or Software Licenses under this Task Order. There is a possibility that Contractors that have OEM Value Added Reseller (VAR) agreements may create a current or subsequent Organizational Conflict of Interests (OCI) as defined in FAR Subpart 9.5. Contractors shall implement measure to ensure there are no conflicts of interest with recommendations provided. The contractor shall address the plan for OCI in the LCIQCP. (Deliverable # 3, Attachment 1)

The Contractor shall notify the Contracting Officer immediately whenever it becomes aware that there may be an actual or potential OCI based on the work it is performing and shall promptly submit a plan to the Contracting Officer to avoid or mitigate any such OCI. The Contractor's mitigation plan will be determined to be acceptable solely at the discretion of the Contracting Officer and in the event the Contracting Officer unilaterally determines that any such OCI cannot be satisfactorily avoided or mitigated, the Contracting Officer may affect other remedies as he or she deems necessary, including prohibiting the Contractor from participation in subsequent contracted requirements which may be affected by the OCI.

1.6.16.1 Non-Disclosure Agreements

Work at specific sites or on specific projects mandate the need for Contractor personnel to withhold sensitive information from those not directly working specific tasks. Select contractor personnel may be required to sign non-disclosure agreements by the CORs in order to protect all Government information to which they have access both during and after contract performance completion. The non-disclosure agreements shall specify that The Contractor's personnel shall not disclose Government specified information at any time even to their respective employers. Attachment 13 contains a list of functions for which contractor personnel shall sign Non-Disclosure agreements. The Contractor shall furnish to the Government copies of Non-Disclosure Agreements DoD Directive 5105.21-M-1 prior to employee arrival at specific locations or starting work on specific projects. The Contractor shall post non-disclosure agreements on COR and Contractor controlled access SharePoint web site. (Deliverable # 76, Attachment 1)

1.6.17 War Risk Insurance

In compliance with Federal Acquisition Regulation (FAR), Clause 52.228-4 (Workers' Compensation and War Hazard Insurance Overseas), contractors are required to provide compensation insurance for their US personnel who are subject to the War Hazards Compensation Act. As such, the Contractor may elect to be reimbursed by the government for the cost of this insurance. Most insurance companies consider Colombia to be a War Risk

Country. The Contractor shall be authorized to provide War Risk Insurance for US citizens in Colombia who support this Task Order.

1.6.18 Phase In/Phase Out Periods

These periods cover all stages of performance for tasks required to transfer responsibility for support of the existing services from the incumbent Contractors to the new Contractor in a collaborative and helpful manner. To minimize any decreases in productivity and to prevent possible negative impacts on services, the Contractor shall have a phase-in planning team on board, during the phase-in/ phase out periods for each respective site/contract. The Government and the Contractor shall validate the time period for the phase-in identified in Attachment 3 at award. During the phase-in period, the Contractor shall become familiar with performance requirements in order to commence full performance of services on the contract start date. The Contractor shall also start planning efforts for consolidation of services and remote management of systems during the phase-in periods as appropriate.

Phase-Out period occurs at the Task Order. The Contractor shall work with a future contractor to transfer responsibility for support of the services under this Task Order to the new Contractor in a collaborative and helpful manner.

1.6.19 Local Nationals

The Contractor may employ local nationals but only in Colombia and Honduras and only for positions that do not require secret clearances. Local Nationals must pass approved local background checks. The Government shall provide instructions and points of contact for local background checks after contract award.

1.6.19.1 Local National Personnel – Adherence to Local Country Laws

For personal hired as local nationals, the Contractor shall comply with all applicable laws of the respective country in which the work is performed. The Contractor shall conduct, establish, incorporate, and register business operations in accordance with the applicable country Commerce Codes. Typically, the codes are written in the local language and readily available on the local government websites under Labor Laws. The Contractor is responsible for performing the required research and adhering to requirements.

1.6.20 Permanent Change of Station (PCS) to JTF-Bravo, JTF-GTMO or a SCO

The tour of duty for U.S. Citizens is PCS; personnel on permanent assignment to JTF-Bravo, JTF-GTMO and SCOs shall not be considered on Temporary Duty (TDY). The Contractor employee may be in unaccompanied status. Reimbursement of dependent travel is not authorized. The Contractor shall be entitled the provisions for PCS cited in the Joint Travel Regulations (JTR).

1.6.20.1 Household Goods and Privately Owned Vehicles (POVs) to JTF-GTMO

The Government has pre-arranged bulk shipment contracts with large carriers. The Contractor is authorized to use available Government transportation to ship household goods and POVs from NAS Jacksonville, Florida to USNB Guantanamo Bay, Cuba at travel discount rates in accordance with other existing Government contracts and or agreements.

1.6.20.2 Use of Government Facilities and Services at JTF-GTMO

See Attachment 23

1.6.20.3 Use of Government Facilities and Services at JTF-Bravo

See Attachment 22

1.6.20.4 Travel to JTF-GTMO

Use of military air for travel to JTF-GTMO is authorized. The Contractor shall use military air travel when commercial air is not available, or when the use of military air by the Contractor is more cost effective for the Government. The Contractor shall submit both options for COR or ACOR approval prior to travel.

1.6.20.5 Personnel Vacancy for JTF-Bravo, JTF-GTMO, or SCOs

If a position has been filled for a consecutive 12- month period and then becomes vacant, the Government will reimburse the Contractor for the PCS costs to relocate that person or persons who will be a permanent employee for the vacant position(s). The Contractor shall replace, at no cost to the Government, personnel who do not complete the 12 month minimum tour lengths.

1.6.21 Access to Strategic or Fiscal Planning Government Systems

In accordance with DoD Directive Number 7045.14, dated 21 November 2003, contractors are not allowed access to any DOD system including Program-Planning Budgeting System without explicit authorization of a relevant Government official, and that is based on a need-to-know basis only. Individuals granted access shall have the appropriate clearance for access to a particular system.

1.6.22 Employment Eligibility

The Contractor shall ensure that all personnel performing services under this Task Order have been pre-screened for employment eligibility using the E-verify Program on the Department of

Homeland Security website http://www.uscis.gov/e-verify. Personnel that have not met the employment eligibility requirement on this website are not authorized to perform services under this Task Order. Verification of the eligibility check will be made available to the KO or COR upon request. This requirement is not in lieu of and does not relieve the Contractor from the I-9 Employment Eligibility Verification Forms for employment of personnel.

PART 2

DEFINITIONS & ACRONYMS

2. DEFINITIONS AND ACRONYMS

2.1 Definitions

2.1.1 Application Management

Application Management is the process responsible for lifecycle of applications (requirements, development, build, deployment, operation, optimization, and retirement) in support of administrative or operational functions and missions.

2.1.2 Best Effort

That effort expended by The Contractor to perform within the awarded ceiling price all work specified in this Task Order and all other obligations under this Task Order. This effort includes providing required qualified personnel, properly supervised, and following industry accepted methodologies and other practices. The effort is further characterized by operating at all times with the Government's best interest in mind, using efficient and effective methods, and demonstrating sound cost control. The effort shall be identical to the effort that would be expended if this were a firm-fixed price contract and The Contractor's profits were dependent upon reducing costs while meeting the Government's requirements in terms and quality and schedule. Failure to provide this required effort may result in the withholding of payment for hours expended that do not qualify as best effort or a reduction in the rate per hour to reflect decreased value of services received.

2.1.3 Original Equipment Manufacturer (OEM) Gold Certified Partners.

OEM Gold Certified Partners are OEM accredited independent technical support providers. These entities often offer a comprehensive range of support for OEM products.

2.1.4 Contractor

The prime Contractor is the entity signing the contract. When the term "contractor" is used in relation to obligations under the contract, the term includes any person, organization, or entity employed or used by the prime contractor to execute its responsibilities.

2.1.5 Contracting Officer

Reference DFARS 202.101. A person with authority to enter into, administer, and or terminate contracts, and make related determinations and findings on behalf of the government. Note: The only individual who can legally bind the government.

2.1.6 Contracting Officers Representative (COR)

Reference DFARS 202.101. An employee of the U.S. Government appointed by the contracting officer to administer the contract. Such appointment shall be in writing and shall state the scope of authority and limitations. This individual has authority to provide technical direction to The Contractor as long as that direction is within the scope of the contract and their designation letter, does not constitute a change, and has no funding implications. This individual does NOT have authority to change the terms and conditions of the contract.

2.1.7 Contractors Authorized to Accompany the Force (CAAF).

Contractor personnel, including all tiers of subcontractor personnel, who are authorized to accompany U.S. Armed Forces in applicable operations and have been afforded CAAF status through a letter of authorization. CAAF generally include all U.S. citizen and third-country national personnel not normally residing within the operational area whose area of performance is in the direct vicinity of U.S. Armed Forces and who routinely are collocated with the U.S. Armed Forces (especially in non-permissive environments).

2.1.8 Core Data Center

A Core Data Center (CDC) is a fixed DoD data center meeting DoD standards for facility and network infrastructure, cybersecurity, technology, and operations and adhering to enterprise governance. CDCs are fundamental components of Department's/Agency's post consolidation environment. Core Data Centers serve as primary consolidation points for enterprise IT services allowing the DoD to achieve economies of scale and deliver the lowest possible Cost per Operating System per Hour (COSH). CDCs have sufficient power and cooling to support anticipated operations, appropriate redundancy to meet availability requirements, adequate space for anticipated growth, and appropriate level of physical security, support delivery of IT services for a diverse community of customers over a wide geographic area, and comply with Federal and industry best practices for energy efficiency and operations.

2.1.9 Defective Service

A service output that does not meet the standard of performance associated with the Performance Work Statement.

2.1.10 Deliverable

Information in the form of documentation to include reports, status, designs, checklists, plans, procedures, that is required to be physically or electronically delivered.

2.1.11 Deprecate, Deprecation or Deprecated

Deprecate or deprecation is the process of replacing information technology or associated functions or capability by others. Deprecated refers to functions or information technology elements that have been replaced by others.

2.1.12 Engineering

Engineering is the process responsible for designing, building, and maintaining services and products, to include supporting systems and infrastructure, (hardware and software,). The systems and services must perform and function as required by the administrative or mission User/sponsor, allow for standardized integration into the architecture, meet agreed levels of reliability and availability, maintain data integrity, and be secure. Systems engineering may be the term used for the organizational element that is responsible for engineering.

2.1.13 Geographically Separated Unit

Geographically Separated Unit (GSU) is a fixed location with no functionality to an installation should it become disconnected from the enterprise. There is no application hosting or data processing in an ISN. There are no services such as Active Directory servers, Domain Name Service (DNS) servers, Assured Compliance Assessment Solution servers, Host Based Security System servers, and print servers. GSUs reach pack to IPNs or ISNs for service.

2.1.14 Hoteled Systems

A Hoteled System is one that is under the technical and program management control of another organization but is provided Domain Name Service (DNS), network connectivity, as well as, space, power, and cooling support by a host organization.

2.1.15 Installation Processing Node

An Installation Processing Node (IPN) is a fixed DoD data center serving a single DoD installation and local area (installations physically or logically behind the network boundary) with local services that cannot be (technically or economically) provided from a CDC. There will be no more than one IPN per DoD installation, but each IPN may have multiple enclaves in order to accommodate unique installation needs (e.g., joint bases). IPNs provide general purpose processing and storage capability for any applications which have a requirement to be locally hosted; this includes enterprise services which must be extended to the installation. CDCs are the default location for hosting all applications, services, and data; applications and data maintained at an IPN should only be for mission necessity. When applicable, this data should be synchronized with data hosted in the CDC environment in order to ensure a single authoritative source.

2.1.16 Installation Service Node

An Installation Services Node (ISN) is a location with the localized equipment necessary to provide the minimum basic functionality to an installation should it become disconnected from the enterprise. There is no application hosting or data processing in an ISN. Potential services include read only Active Directory servers, Domain Name Service (DNS) servers, Assured Compliance Assessment Solution servers, Host Based Security System servers, and print

servers. In addition, ISNs may host UC capabilities that must remain on the installation to enable emergency services even when the connection is interrupted.

2.1.17 Key Personnel

Contractor personnel that may be required to be used in the performance of the contract by the Key Personnel provision listed in the PWS.

2.1.18 Non-CAAF

Personnel who are not designated as CAAF, such as local national (LN) personnel and non-LN personnel who are permanent residents in the operational area or third-country nationals not routinely residing with U.S. Armed Forces (and third-country national expatriates who are permanent residents in the operational area) who perform support functions away from the close proximity of, and do not reside with, U.S. Armed Forces.

2.1.19 Original Equipment Manufacturer (OEM)

An OEM is a company whose products are used as components in another company's product or services. The OEM will generally work closely with the company that sells or maintains the finished product (the latter often called a "value-added reseller" or VAR) and customize the designs based on the customer needs.

2.1.20 Physical Security

Actions that prevent the loss or damage of Government property.

2.1.21 Quality Assurance Surveillance Plan (QASP)

The Quality Assurance Surveillance Plan (QASP) is the key Government-developed surveillance process document that is applied to Performance-Based Service Contracting (PBSC) and is used to manage contractor performance assessment by ensuring that systematic quality assurance methods are utilized to validate that the contractor's quality control efforts are timely, effective, and are delivering the results specified in the contract or task order.

2.1.22 Quality Control

All necessary measures taken by The Contractor to assure that the quality of an end product or service shall meet contract requirements.

2.1.23 Response Time

Response time is the time elapsed between when the incident or malfunction is identified to the time a technician is working the problem on site.

2.1.24 Security Stack

A security stack is a general term for the serial or parallel integrated set of cybersecurity tools systems to include firewalls, Intrusion Detection Systems, Intrusion Prevention Systems, Vulnerability Scanning systems, Security Information Management system, Content Filtering, Correlation Systems, Malware protection systems, application and device control systems.

2.1.25 Sensitive Compartmented Information (SCI) Indoctrination

SCI indoctrination means providing a briefing related to the handling and protection of SCI related information or material and having that individual accept responsibility for handling and protecting that information.

2.1.26 Service Desk

The Service Desk acts as the single primary point of contact (i.e. the interface) between the user and the service. If there is an issue whether it be an unclear Event or Alert message, an Incident or Problem, or an Access issue, the user is going to contact the Service Desk for assistance if the issue cannot be resolved through self-help methods.

The purpose of the Service Desk is to:

Be primary contact point for all calls, questions, service requests, complaints, and remarks.
Be primary provider of ongoing monitoring and management of mission partner satisfaction through appropriate communication channels. Manage the incident lifecycle.
As other processes mature, the Service Desk becomes more involved in areas such as Configuration Management, but the primary purposes above remain the same.

2.1.27 Service Operations

The Service Operations is related to the full range of matters pertaining to sustaining assured information delivery, system and network availability, and information protection for information technology (IT) capabilities that support the provided services. Service Operations entails introducing new initiatives, ensures standards-based configuration and operation of all infrastructure, control of runtime aspects of services to ensure services behave correctly and within SLAs, administration and control of security policies, identification of incidents and infrastructure issues, performing problem resolution, and implementing metrics that track the overall progress of the operations. The Service Operations Manager shall ensure that processes that support services are executed in a cost-effective manner and measure the effectiveness of controls to determine how well the controls achieved the planned control objectives.

2.1.28 Subcontractor

One that enters into a contract with a prime contractor. The Government does not have privity of contract with the subcontractor.

2.1.29 Tier/Level 1 (T1/L1)

This is the initial support level responsible for basic customer issues. It is synonymous with first-line support, level 1 support, front-end support, support line 1, and various other headings denoting basic level technical support functions. The first job of a Tier I specialist is to gather the customer's information and to determine the customer's issue by analyzing the symptoms and figuring out the underlying problem. When analyzing the symptoms, it is important for the technician to identify what the customer is trying to accomplish so that time is not wasted on "attempting to solve a symptom instead of a problem."

2.1.30 Tier/Level 2 (T2/L2)

This is a more in-depth technical support level than Tier I and therefore costs more as the techs are more experienced and knowledgeable on a particular product or service. It is synonymous with level 2 support, support line 2, administrative level support, and various other headings denoting advanced technical troubleshooting and analysis methods. Technicians in this realm of knowledge are responsible for assisting Tier I personnel in solving basic technical problems and for investigating elevated issues by confirming the validity of the problem and seeking for known solutions related to these more complex issues.

This team usually collects information such as program name that is failed or application name or any database related details (table name, view name, package name, etc.) or API names. These details are useful for Tier 3.

If a problem is new and/or personnel from this group cannot determine a solution, they are responsible for raising this issue to the Tier III technical support group.

2.1.31 Tier/Level 3 (T3/L3)

This is the highest level of support in a three-tiered technical support model responsible for handling the most difficult or advanced problems. These individuals are experts in their fields and are responsible for not only assisting both Tier I and Tier II personnel, but with the research and development of solutions to new or unknown issues. This team can analyze the code and data using information from Tiers 1 and 2.

In some instances, an issue may be so problematic to the point where the product cannot be salvaged and must be replaced. Such extreme problems are also sent to the original developers for in-depth analysis. If it is determined that a problem can be solved, this group is responsible

for designing and developing one or more courses of action, evaluating each of these courses in a test case environment, and implementing the best solution to the problem. Once the solution is verified, it is delivered to the customer and made available for future troubleshooting and analysis.

2.1.32 Tier/Level 4 (T4/L4)

While not universally used, a fourth level often represents an escalation point beyond the normal operations and maintenance organization. This is either systems engineering (responsible for implementing new capabilities) or generally a hardware or software consulting vendor or an OEM Gold Certified Partner. Within a corporate incident management system it is important to continue to track incidents even when they are being actioned by a vendor and the Service Level Agreement (SLA) may have specific provision for this.

2.1.33 Work Day

The number of hours per day The Contractor provides services in accordance with the contract.

2.1.34 Work Week

Monday through Friday, unless specified otherwise.

2.1.35 Virtual Local Area Network (V-LAN)

V-LAN is a LAN where is a single layer-2 network is partitioned to create multiple distinct broadcast domains, which are mutually isolated so that packets can only pass between them via one or more routers.

2.2. Acronyms

AC	Air Conditioning
ACOR	Assistant Contracting Officer's Representative
ADPE	Automated Data Processing Equipment
ADS	Anomaly Detection System
AFARS	Army Federal Acquisition Regulation Supplement
AIS	Automated Information Systems
AKO	Army Knowledge Online
AMD	Asset Management Database
AOF	Area of Focus
AOR	Area of Responsibility
APAN	All Partners Access Network
APMS	Army Portfolio Management Solution

AR	Army Regulation
ARs	Army Regulations
asreq	As Required
ATS	automatic transfer switches
BBS	Batch-Broker Service
C&A	Certification and Accreditation
C2PC	Command and Control PC
C4I	Command, Control, Communications, Computers, and Information Systems
C4S	Command, Control, Communications, and Computer Systems
CAA	Controlled Access Area
CAAF	Contractor Authorized to Accompany the Force
CAC	Common Access Card
CAMs	Coordinated Alert Messages
CAP	Contractor Acquired Property
CAPCM	Certification and Accreditation Professional Manager
CATAM	Comando Aereo de Transporte Militar
CBT	Computer Based Training
CCB	Configuration Control Board
CCCB	Configuration Control and Change Control Board
CCCE-W	CECOM Contracting Center – Washington
CCE	Contracting Center of Excellence
CCI	Controlled Cryptographic Item
CCIB	Command and Control Interoperability Board
CD	compact disk
CDRL	Contract Data Requirements List
CDS	Cross Domain Solution
CENTRIXS	Combined Enterprise Regional Information Exchange System
CFR	Code of Federal Regulations
CILA	Colombian Imagery Library Architecture
CISMOA	Communication Interoperability and Security Memorandum of Agreement
CISSP	Certified Information System Security Professional
CJCSM	Chairman of the Joint Chiefs of Staff Manual
CM	Contract Manager
CMEs	Contractor Manpower Equivalents
CMI	classified message incidents
CMP	Configuration Management Plan
CMR	CONTRACTOR MANAGEMENT REPORTING
CMRA	Contractor Manpower Reporting Application
CND	Computer Network Defense
COCO	Contractor Owned Contractor Operated
COMSEC	Communications Security
CONAUTH	Controlling Authority
CONOPS	Concept of Operations

CONUS	Continental United States
COP	Common Operational Picture
COR	Contracting Officer Representative
COTS	Commercial-Off-the-Shelf
CPEs	Professional Education credits
CPM	Contractor Program Manager
CPU	central processing unit
CRR	COMSEC Release Request
CS	Cyber Services
CSD-E	Contractor Support Detachment-East
CSII	Cooperating Sensor Information Integration
CSS	Control of Communications Security
CTOs	Communications Tasking Orders
DA	Department of the Army
DAA	Designated Approval Authority
DAA's	Designated Approval Authority
DAC	Department of the Army Civilians
DAO	Defense Attaché Office
DASD-CN	Deputy Assistant Secretary of Defense for Counternarcotics
DAT	Digital Audio Tape
DCS	Defense Courier Service
DD250	Department of Defense Form 250 (Receiving Report)
DD254	Department of Defense Contract Security Requirement List
DESMF	DoD Enterprise Service Management Framework
DFARS	Defense Federal Acquisition Regulation Supplement
DHCP	Dynamic Host Control Protocol
DIACAP	DOD Information Assurance Certification and Accreditation Process
DIAS	Distributed INFOSEC Accounting System
DISA	Defense Information Systems Agency
DMDC	Defense Manpower Data Center
DNS	Domain Name Service
DOD	Department of Defense
DODAAC	Department of Defense Activity Address Code
DODIIS	Department of Defense Intelligence Information System
DOIM	Director of Information Management
DoS	Department of State
DRMO	Defense Reutilization Management Office
DTS-PO	Defense Telecommunications Services Program Office
DVD	Digital Versatile Disc
ECV	Enhanced Compliance Visits
EITSSC	Enterprise Information Technology Services Support Contract
EKMS	Electronic Key Management System
ELA	Enterprise License Agreement

eMASS	Enterprise Mission Assurance Support System
EOIP	Everything Over IP
ES	Enterprise Support
FAQs	Frequently Asked Questions
FAR	Federal Acquisition Regulation
FFP	Technical Control Facility
FISMA	Federal Information Security Management Act
FOC	Full Operational Capability
FOUO	For Official Use Only
FRAGOs	Fragmentation Orders
FSC	Federal Service Code
FSO	Facility Security Officer
GCCS	Global Command and Control Systems
GCCS-J	Global Command and Control Systems-Joint
GCSS-Army	Global Combat Support System - Army
GFE	Government Furnished Equipment
GFP	Government Furnished Property
GIAP	GIG Interconnection Approval Process
GIG	Global Information Grid
GO	General Officers
GOCO	Government Owned Contractor Operated
GOGO	Government Owned Government Operated
GOTS	Government of the Shelf
GPC	government purchase card
GSA	General Services Administration
GSUs	Geographically Separated Units
GTL	Government Task Lead
HAIPE	High Assurance Internet Protocol Encryptor
HBSS	Host Base Security System
HF	High frequency
HIPAA	Health Insurance Portability and Accountability Act of 1996
HNA	host nation approvals
HQ	Headquarters
IA	Information Assurance
IAMS	Information Assurance Management System
IAP	Information Assurance Program
IAR	Information Assurance Reviews
IAT	Information Assurance Technical Level
IATC	Interim Authority To Connect
IATO	Initial Authority To Operate
IAVA	Information Assurance Vulnerability Assessment
IAVB	Information Assurance Vulnerability Bulletins
IAVM	Information Assurance Vulnerability Management

ICP	Inside Cable Plant
IdAM	Identity and Access Management
IDS	Intrusion Detection System
IdSS	Identity Synchronization Service
IGCE	Independent Government Cost Estimate
ILS	Integrated Logistics Support
ILSP	Integrated Logistics Support Plan
IM	information management
IMO	Information Management Officer
IMS	Information Management Systems
INFOCON	Information Conditions
INFOSEC	Information Security
IP	Internet Protocol
IPN	Installation Processing Node
IPS	Intrusion Prevention Systems
ISN	Installation Service Nodes
ISOPREP	Isolated Personnel Report
ISP	Internet Service Provider
ISSM	Information System Security Manager
ISSO	Information Systems Security Officer
IT	Information Technology
ITO	Information Technology Officer
ITOs	Information Technology Officer
ITR	Information Technology Request
J6	Joint Communications
JC2	Joint Command and Control
JCC	Joint Cyber Center
JIATF-S	Joint interagency task force south
JIE	Joint Information Environment
JPAS	Joint Personnel Adjudication System
JTF	Joint Task Force
JTF-GNO	Joint Task Force-Global Network Operations
JTR	Joint Travel Regulation
JWICS	Joint Worldwide Intelligence Communications System
KEYMAT	Keying Material
KM	Key Management
KO	Contracting Officer
KPIs	Key Performance Indicators
LAN	Local Area Network
LCMC	Life Cycle Management Command
LCMS	Local COMSEC Management Software
LRU	Lowest Replaceable Unit
MANPRINT	Manpower and Personnel Integration

MILGP	Military Group
MNIS	Multi-National Information Sharing
N/A	Non Applicable
NAP	Network Access Point
NDA	national defense area
NIPRNET	Non-Secure Internet Protocol Router Network
NISPOM	National Industrial Security Program Operating Manual
Non-SCI	Non Sensitive Compartmented Information
NSA	National Security Agency
NSC	Node Site Coordinator
O&M	Operation and Maintenance
OCI	Organizational Conflict of Interest
OCONUS	Outside Continental United States
OCP	Outside Cable Plant
ODC	Other Direct Cost
OEM	Original Equipment Manufacturer
OI	Operational Instruction
OPLANS	Operation Plans
OPSEC	Operations Security
OSTR	On-Site Technical Representative
PAT	Planning Assistance Team
PBO	Property Book Office
PBUSE	Property Book Unit Supply Enhanced Property Accounting System
PCA	Physical Configuration Audit
PCMCIA	Personal Computer Memory Card International Association
PCS	Permanent Change of Station
PDAs	personal digital assistant
PDS	Protected Distribution System
PIPO	Phase In/Phase Out
PKI	Public Key Infrastructure
PN	Participating Nation
PNN	Participating Nations Network
POA&M	Plan of Action and Milestones
POC	Point of Contact
POM	program objective memorandum
POR	Program of Record
POTS	Plain Old Telephone Systems
POV	Privately Owned Vehicles
PPS	Ports, Protocols, and Services
PRS	Performance Requirements Summary
PWS	Performance Work Statement
QA	Quality Assurance
QAP	Quality Assurance Program

QASP	Quality Assurance Surveillance Plan
QC	Quality Control
LCIQCP	Quality Control Program
QDR	Quality Deficiency Report
RAD	Rapid Application Development
RAM	Reliability, Availability, and Maintainability
RBS	Real-time Broker Service
REM	Retina Enterprise Management
REMEDYARS	Remedy Action Request System
RMF	Risk Management Framework
RSO	Regional Security Officer
SaaS	Software as a Service
SAV	Staff Assistance Visits
SBU	Sensitive But Unclassified
SC	USSOUTHCOM
SCCMA	SOUTHCOM COMSEC Management Activity
SCI	Security Compartmented Information
SCIFS	Sensitive Compartmented Information Facilities
SCIP	Secure Communication Interoperable Protocol
SCO	Security Cooperation Office
SECTERA	Secure Voice
SEI	Software Engineering and Integration
SES's	Senior Service Executives
SI	special intelligence
SI/TK	Special Intelligence/Talent Keyhole
SILOG	Sistema de Sinergia Logística
SIPRNET	SECRET Internet Protocol Router Network
SLA	Service Level Agreement
SOFA	Status of Forces Agreements
SOP	Standard Operating Procedure
SPOT	Synchronized Predeployment and Operational Tracker
SSA	Security Architecture
SSCP	Systems Security Certified Practitioner
STE	Secure Telephone Equipment
STIG	Security Technical Implementation Guides
SWG	Spares Working Group
T&M	Time & Material
TAC	Transportation Account Code
TB	Technical Bulletin
TCF	Tech Control Facility
TCI	Technical Counterintelligence
TCO	Telephone Control Officer
TDY	Temporary Duty

TE	Technical Exhibit
Telco	Telecommunications Company
TESA	Technical Expert Status Accreditation
TNCC	Theater Network Coordination Center
TO	Task Order
TS	Top Secret
TTP	Tactics, Techniques, and Procedures
UC	Unified Capabilities
UHF	ultrahigh frequency
UIC	Unit Identification Code
UPS	Uninterruptible Power System
USNORTHCOM	United States Northern Command
USSOUTHCOM	United States Southern Command
VHF	Very High Frequency
VMS	Vulnerability Management System
VoIP	voice-over-IP
V-LAN	Virtual LAN
VPN	Virtual Private Network
VSAT	Very Small Aperture Terminal
WAN	Wide Area Network
WBT	Web Based Training
XML	Extensible Markup Language

PART 3

GOVERNMENT FURNISHED PROPERTY, EQUIPMENT, AND SERVICES

3. GOVERNMENT FURNISHED ITEMS AND SERVICES

3.1. Services

The Government will provide all DoD Information Network (DoDIN) interconnectivity (NIPRNET/SIPRNET/INTERNET/ JWICS) and telephone services from appropriate service providers to accomplish the tasks in this Task Order. The Government may also provide other services to include planning, designing, transition, or support services from other Government agencies or contractors, as well as OEM support and integration of new capabilities.

3.2 Facilities

With the exception of the required Contractor furnished and the Government reimbursable warehouse in Doral Florida, the Government will furnish the necessary workspace and equipment space for the Contractor staff to provide the support outlined in this PWS.

3.3 Utilities

The Government will provide all utilities to include power and cooling in facilities made available for the Contractor's use in performance of duties outlined in this PWS unless otherwise specified. The Contractor shall instruct personnel in utilities conservation practices. The Contractor shall be responsible for operating under conditions that preclude the waste of utilities which include turning off the water faucets or valves after using the required amount to accomplish cleaning vehicles and equipment.

3.4 Government Furnished Equipment (GFE)

The Government shall provide all equipment on this effort as GFE. The Contractor shall address how they shall manage and track all GFE, to include creating and maintaining lists for accountability of all GFE in the LCIQCP. The Contractor shall maintain a list of all GFE available for inspection at any time. (Deliverable # 3, Attachment 1)

3.4.1 Administrative Support Equipment

The Government will provide telephones, computer equipment (to include all necessary hardware & software), and associated peripheral devices, facsimile machines, copier, and other basic office supplies required to complete the work described in the PWS. The Contractor shall ensure that contractor proprietary information is not stored on government furnished computers, databases, web-portals, or transmitted vial Government email systems. The Contractor shall

implement processes and procedures at their own costs, to ensure that personnel do not leave contractor proprietary information on Government Furnished computers or applications; Contractor shall address these processes in the LCIQCP. The Government will not be responsible for any proprietary information transferred to other companies as a result of contractor personnel transfers or turnovers. All information stored, developed, and transmitted on Government computers and or applications shall be considered as property of the Government and may be used in any manner required. (Deliverable # 3 Attachment 1)

3.4.2 GFE Information Technology (IT) Equipment

The Government will provide access all IT Equipment and associated test equipment for the Contractor to accomplish the required work. For the purpose of this Task Order, three types of GFE shall receive special consideration: Supported Systems/Equipment, Ancillary Equipment, and GFE. GFE includes powered and non-powered tools, equipment; administrative equipment; and test, measurement and diagnostic equipment (TMDE). The Government will replace any Supported System/Equipment or Ancillary Equipment that becomes uneconomically repairable (as determined by the Government) at the Government's discretion and expense. The Contractor shall not use GFE for any purpose other than in the performance of this Task Order. Any Government-owned TMDE provided to the contractor as GFE will be calibrated by the contractor at Government expense in accordance with applicable DoD calibration schedules. The Government will issue user identification and passwords for access to GFE networks IAW established procedures. The Contractor shall document and maintain a list of all GFE equipment. (Deliverable # 9 Attachment 1)

3.4.3 Contractor Acquired Property

All equipment procured by the Contractor with COR approval and Government funds shall be considered Contractor Acquired Property (CAP) and shall be considered GFE upon receipt. Any GFE, acquired shall revert to the US Government at the conclusion of this Task Order. All CAP shall be added to the Contractor's sub-hand receipt. All purchased material, hardware, and/or software product shall become the property of the Government upon delivery.

3.4.4 Replacement of GFE

The Government is not required to replace GFE provided on an as-is basis unless that equipment cannot support its intended function. The Contractor shall replace such equipment, if necessary, to ensure full and continued performance of the requirements of this Task Order.

3.4.5 Disposition of Replaced / Unserviceable Parts

The Contractor shall turn in any parts, components or assets that are replaced due to lack of functionality to the Defense Material Reutilization Office (DRMO). The Contractor shall coordinate with the COR and Property Book Officer before turning in equipment or components

to DRMO. The Contractor shall maintain a log of all equipment or components turned into DRMO. (Deliverable # 77, Attachment 1)

3.5 Materials and Information

The Government will furnish all available equipment baselines, engineering drawings, interconnection diagrams, circuit diagrams, and floor plans, operating procedures, or policies after award. The Government will issue user identification and passwords to Government networks IAW established procedures. The Government will provide any software design documents, access to source code and libraries, and previously developed training software (Computer-based training, or web-based training packages) and all PowerPoint and paper-based materials, such as manuals. The Government does not guarantee the accuracy of this information provided. The Contractor shall be responsible for identifying any inaccuracies as part of their review during the phase-in period as well as updating or creating new documentation to reflect accurate installation and configuration of items in accordance with paragraph 5.1.1.1 and 5.1.1.1.1.

3.6. Organizational Information

The Government will provide all contractor personnel with initial orientation / familiarization on the Government's organizational structure. Basic information on HQ SOUTHCOM can be found on the following homepages.

http://www.southcom.mil/aboutus/Pages/About-Us.aspx

Information on other organizations supported by this effort can be found here:

http://www.southcom.mil/aboutus/Pages/Our-Team.aspx

PART 4

CONTRACTOR FURNISHED ITEMS AND SERVICES

4. CONTRACTOR FURNISHED ITEMS AND RESPONSIBILITIES

4.1 General

The Contractor shall furnish all supplies, equipment, facilities and services required to perform work under this Task Order that are not listed under Section 3 of this PWS.

4.2 Facility Clearance, Employee Security Clearances, and Related Requirements

The security requirements for this task are defined in the attached DD254. The Contractor Facility Security Officer (FSO) shall provide a plan for contractor personnel to obtain their security badges during the phase-in period through the Security Office of each location in this PWS.

The Contractor shall possess and maintain a TOP SECRET facility clearance from the Defense Security Service with no safeguarding for offsite requirements. The highest level of security clearance requirement for this Task Order is Top Secret (TS) with Sensitive Compartmented Information (SCI) access of sensitive information/talent keyhole (SI/TK). All US Citizen personnel shall possess an interim or permanent Secret or Top Secret/Sensitive Compartmented Information (TS/SCI) security clearance prior to starting work on this effort. The security clearance must match the level of support before starting work on this effort.

The Contractor shall be provided access to COMSEC information, Sensitive Compartmented Information (SCI), NON-SCI intelligence information, NATO information, and For Official Use Only (FOUO) information. Due to the nature of this effort, certain Contractor shall also have access to Privacy Act, Finance, and contract related information as a result of elevated permissions on the information systems. The Contractor shall be provided access to the SIPRNET system. The Contractor shall be required to access Special Access Program (SAP) at designated locations.

In accordance with Technical Specifications (IC Tech Spec-for ICD/ICS 705, page 63) for Construction and Management of Sensitive Compartmented Information Facilities (SCIFS), Contractor personnel with elevated permissions to Access Control Systems (example: Security Management Databases, Human Resource/Personnel Management Systems, etc.), shall be SCI Indoctrinated by an SC-approved government organization.

Given the duties and information access required, appropriate Contractor personnel supporting Software Engineering and Integration (SEI) or the Theater Network Coordination Center

(TNCC), require indoctrination into Focal Point Program (FPP)/Alternate or Compensatory Control Measure (ACCM) Control Programs.

FPP/ACCM Access Required. Individuals working with ACCM/FPP require additional training on the handling and safeguarding of ACCM/FP material and shall comply with the following:

REQUIRED FOR ON-SITE ONLY

(1) All ACCM/FPP work will be done "onsite" at the government facility. No ACCM/FFP material will be stored/transferred/viewed at the contractor facility.

(2) The contractor will safeguard all ACCM/FPP information in accordance with CJCSM 3213.02 Series, "Joint Staff Focal Point Program" and the Program Security Plan and Security Classification Guide for the specific program(s).

REQUIRED FOR OFF-SITE ONLY. All ACCM/FPP work will be done in a government-approved facility. Approval shall be granted by appropriate FPP Control Office (FPPCO).

(1) The FPPCO will coordinate identification of the authorized users for each Focal Point (FP) program processed by the contractor. Access to the ACCM/FPP information shall be limited to only those with a specific association with operational task, mission, or specific contract deliverable.

(2) A list of authorized users shall be maintained as an Access Control List (ACL), which will define the individuals or groups, granted access to ACCM/FPP information. A record of each ACL, and any changes, shall be maintained during the duration of the contractor's involvement in the ACCM/FPP and will be filed with the government FPPCO when the contract is terminated.

(3) Systems processing ACCM/FPP information must provide Need-To-Know (NTK) enforcement based on a Discretionary Access Control (DAC) policy that establishes a security structure that defines and controls access between users and objects (e.g. data/information, files, and programs) in the system. Use of a single "group" ID with a single password is not authorized for control of access to ACCM/FPP information. The FPPCO shall control and verify the establishment and function of DACs on the contractor's information system before it is used to process ACM/FPP information.

Foreign National contracted services may be required by certain partner nation agreements or be in the best interest of the Government. The Contractor shall vet and clear all Foreign Nationals via the local US Embassy Regional Security Office. The COR will facilitate this process upon identification of local foreign nationals.

4.2.1 Visit Certifications

The Contractor shall submit visit certifications for all personnel visiting Government facilities. See Attachment 4 for specific instructions to send visit Certifications.

4.2.2 Notification of Personnel working on this Task Order

In addition to visit certifications that must be sent by appropriate Facility Security Officers, the Prime Contractor must provide and maintain a current list of all personnel (to include sub-contractor personnel) working on this Task Order that require access to any of the facilities. Contractor personnel whose visit certifications are processed via JPAS (Joint Personnel Adjudication System) but that are not on identified through formal notification to the COR, will not be processed for permanent badges or non-escort visitor badges. (See Deliverable # 2, 73 Attachment 1)

4.3. Materials to include Drawings, Diagrams, Plans, Procedures, Policies, and Other Systems Documents

The Contractor shall develop updates and maintain current all materials provided by the Government as required by appropriate tasks in this PWS. This includes engineering drawings, system requirements or description documents, interconnection diagrams, circuit diagrams, and floor plans, operating procedures, or policies. The Government will issue user identification and passwords to Government networks IAW established procedures. The Government will provide available software design documents, access to source code and libraries, and previously developed training software (Computer-based training, or web-based training packages) and all PowerPoint and paper-based materials. The Government shall make available all existing documentation related to the following attachments during the Phase-In period.

Attachment 4 - Infrastructure and Systems Identified in APMS
Attachment 5 - Security Requirements by Functional Area and Clearance Certifications
Attachment 6 - Networks & Systems Under This Effort
Attachment 9 - Services by Location
Attachment 10 - Maintained, Hosted, or Hoteled User Web Based or Command and Control Government Developed Applications
Attachment 11 – JIE Technical Implementation Guidelines
Attachment 14 – Summary of PC, Servers and Applications on Servers By Location
Attachment 15 – VSAT Systems and Locations
Attachment 16 – MNIS and CENTRIXS Locations
Attachment 17 – Internet Service Provider Locations
Attachment 18 – Life Cycle Related Projects
Attachment 19 – Level 1 and Level 2 Information Assurance Accreditation Package Work
Attachment 20 – Maintained Software Applications
Attachment 21 – Organizational Background Information
Attachment 22 - JTF-Bravo Unique Services
Attachment 23 - JTF-GTMO Unique Services
Attachment 24 - Software Engineering and Integration
Attachment 25 - Defense Cyber Operations and NetOps Tool Sets

Attachment 26 - Generic Network Diagram (Actual Drawings)

4.3.1 Classified Material

The Contractor shall properly safeguard all generated or GFE classified material in accordance with applicable regulations outlined in the DD Form 254.

4.3.2 Information Systems Security

The Contractor shall protect Government networks based on the level of access provided to Contractor personnel supporting this Task Order. The Contractor shall apply and enforce information assurance measures, such as personnel, physical, and communications security procedures, required by AR 25-2 posted as of the date of Contract Award and other Cyber Security Documents on this Task Order. The Contractor shall ensure that personnel in these positions acquire and maintain appropriate security clearances, background investigations, and IA training as specified by AR 25-2.

4.3.2.1 Safeguarding public key infrastructure (PKI) Tokens

The Contractor shall take appropriate measures to safeguard their Government-issued security badges, common access cards (CAC), and SIPRNET PKI Tokens as outlined in USSOUTHCOM HQ's security policies and other applicable regulations.

4.4. Equipment

All equipment under this Task Order shall be considered Government Furnished Equipment. The Contractor shall not furnish any equipment on their own.

4.5 Drug Testing

Positions with a Secret or higher clearance level are subject to testing for illegal drug use. The Contractor shall follow DoD Federal Acquisition Regulation Supplement (DFARS) clause 252.223-7004, Drug-free Work Force; and local USSOUTHCOM policies regarding drug testing. The Contractor shall perform drug tests, ensuring all Secret-cleared contractor personnel are tested at least once a year, every year of the TO, as well as when there is a reasonable suspicion that an employee uses illegal drugs, at The Contractor's expense. The Contractor shall report any positive test results to the COR immediately. The Contractor shall make available all records of drug testing to the COR upon request.

4.6 Polygraph Testing

Contractor personnel performing COMSEC support functions may be required to submit to counterintelligence scope polygraph (CSP)screening examination. The COR will provide guidance and direction of this if required.

4.7 Medical Insurance for Work at JTF-GTMO

The Contractor shall retain medical and dental insurance coverage from an insurance carrier accepted by US Naval Base GTMO hospital / medical service providers.

4.8 Common Access Cards and SIPRNET Tokens for Personnel working on this Task Order

The Prime Contractor must provide and maintain a current list of all personnel (to include sub-contractor personnel) working on this Task Order that require Common Access Cards and SIPRNET Tokens. (Deliverable #74 Attachment 1)

PART 5

SPECIFIC TASKS

5 Specific Tasks

The Contractor shall support the Government on all life cycle aspects of IT development, operations, maintenance and use. The Contractor shall assist the Government in developing and executing processes and procedures in accordance with commercial and government best practices for IT life cycle activities and adapted as required to meet the requirements of this PWS. Concurrently, the Contractor shall develop and implement quality control procedures to identify, prevent, and ensure non-recurrence of defective services. The Contractor's quality control program is the means by which they assure their work complies with the requirement of the contract.

The Contractor shall develop an IT Life Cycle Implementation and Quality Control Plan (LCIQCP). The LCIQCP is the main artifact articulating how the Contractor shall accomplish work and meet the performance requirements of this Task Order. Due to the complexity of this program there are several other plans which are considered annexes to the LCIQCP. The LCIQCP shall include a description of the Contractor's team and the organizational structure developed to meet the requirements of the contract. The Contractor shall also provide a list that describes the roles and responsibilities of each organizational structure element, as well as, the composition of each organizational element to include duty title and contract labor category title for each position working on this effort. The organizational structure and the list describing the composition of all organizational elements shall clearly identify the structure/personnel at the beginning of each Phase-In period as well as the changes due to consolidations, network transitions (deprecations), as well as, JIE planning and implementation. When required, the Contractor shall identify organizational structure, composition, duty title and labor categories for organizational elements working on IT Service Corrective Action or New Capability Planning, Design, and Transition or changes to personnel as a result of these modifications. The Contractor shall reference all other deliverables in the LCIQCP. The services provided on this Task Order require deliverables which are either annexes to the LCIQCP or are periodic reports; this list in not all inclusive. See Attachment 1 for a complete list:

Service Area	Required Plans, Assessments, or Reports
Overall	• IT Life Cycle Implementation and Quality Control Plan
	○ Systems Training and Certification List
Service Strategy	• Plan for Assumption of O&M Responsibility
	○ IT Service Corrective Action Assessment
	• JIE Assessments
	• New Capability Assessments
Service Designs	• O&M Transition Designs if Required

	• JIE Designs
	• New Capability Designs
Service Transitions	• O&M Transition Documentation if Required
	• JIE Transition Documentation
	• New Capability Transition Documentation
Service Operations	• IT Service Catalog
	• STIG and IAVM Impact Assessments
	• Service Operations and Maintenance Plan
	• Customer Portable Asset Tracking and Control Database
	○ List of Scripts in Use
	○ List of Hoteled Systems
	○ Telephone System Directory
	• IT Usage Logs if Required
	• COMSEC Inventory Report
	• Cooperating Sensor Information Integration (CSII) Usage Report
	• CSII Sensor Integration Checklist
	• Very Small Aperture Terminal (VSAT) Surveys if Required
	• Minimum Performance Requirements
	• Key Performance Indicators
	• TNCC COMSTAT Report
	• Bandwidth Metrics
Continuous Improvement	• Quality Control Audits
	• Monthly Analysis of Communications Status (COMSTAT) Network Service Call Report, Service Desk Reports, Logs and KPIs
	• Process Improvement Recommendations
Software Engineering and Integration/Application Development	• Hyper-Text Markup Language (HTML)-5 and Token Compliance Report
	• New Application Requirements, Design, and Development Documentation
	• List of Hosted Services
IT Systems Support Services	• Bi-weekly Activities Report
Cyber Security	• Cyber Security Plan
	• Information Condition (INFOCON) and Cyber Tasking Order (CTO) Compliance Report
	• STIG Analysis Report
	• Cyber Readiness Report
	• Vulnerability Scans Report
	• Web Content Filter Report
	• Spyware/Adware Report

	• Incidents Report
	• Network Security Event Log
	• Cyber Security Audit Report
	• Assessment Reports (Daily, Weekly, Monthly, Inspections)
	• COMSEC Reports
SharePoint Activities	▪ SharePoint Activities
Configuration Management	• Software and Hardware Baselines
	System Installation Drawings
	• Physical Configuration Audit Report
	• Functional configuration Audit Report
Procurement	• IT Hardware, Software, Warranties, Licenses, and Expendables Procurement Plan
	• Spares and Consumables List
	• Licenses and Warrantees List
Logistics	• Logistics Support Plan
IT User Support Services	• Training Material
	• SharePoint Activities
IT Consultants and OEM Support Services	• Consultants and OEM Hours Expenditures
On-Call and Emergency Support	• Incident Report
	• Site Recovery Report
	• Fail Over Testing Report
	• Contingency Plan
	• Inclement Weather Plan
Other Reports	• Post Award Conference/Quarterly Progress Briefing
	• Periodic Program Progress, Status, and Management Report
	• Yearly Travel Report
	• Travel Estimate Report
	• Satellite Bandwidth and Internet Service Provider Cost Estimates

The draft LCIQCP is due on submission of the proposal. The Contractor shall deliver updates to this document in accordance with the deliverables breakdown matrix. (Deliverable # 3, Attachment 1)

It is important to note that the term “service” has two distinct meanings in the following paragraphs. One meaning is related to providing a contractual service i.e. to perform work. The other meaning is related a given IT capability i.e. a capability such as voice, video teleconferencing, or specific applications.

Throughout the period of this Task Order, if material discrepancies or conflicting guidance between requirements documents or any verbal communication with a COR or ACOR, are discovered, the Contractor shall notify the COR in writing via a Task Discrepancy Report within one (1) day to obtain resolution. (Deliverable # 12 Attachment 1)

5.1 Basic Services

The Contractor shall provide 9 types of IT related outsourced services in this effort; the first 5 are adapted within the construct of the DoD Enterprise Service Management Framework (DESMF). The Contractor shall address how they will provide and manage all of the services outlined in this paragraph and associated paragraphs in the LCIQCP. Performance measurement for each of these services is addressed in the Government Quality Assurance Surveillance Plan. Performance on this Task Order shall be measured against the Performance Requirements Summary in Attachment 27 using the Quality Assurance Surveillance Plan as described in Attachment 7. (Deliverable # 3 Attachment 1)

- IT Service Strategy and Planning Services (Para 5.1.1 and associated subparagraphs). IT Service Strategy and Planning Services consist of activities required to prepare for a Phase-in or to implement a new capability. For these efforts the Contractor shall assess the operational requirements, translate those requirements in to technical requirements, and develop a detailed plan and cost estimates for follow-on phases for Government approval. Under these services, the Contractor shall coordinate with Government personnel to transition or implement new capabilities. Performance of these services will be measured against ability to meet time (schedule) and labor (costs) proposed by the Contractor to accomplish efforts on a by-task basis. It is expected that this line of effort shall not have resources applied if there are no major services, modifications, or transitions tasked. It is also expected that *some level of* additional expertise to possibly include Consultants, OEM or OEM Certified Gold Partner technical expertise, shall be provided as required in order to ensure appropriate expertise is assigned to these more complex tasks and that personnel performing day-to-day functions are not impacted accomplishing required task.

- IT Service Design Services (Para 5.1.2 and associated subparagraphs). IT Service Design Services consist of activities required to design the capabilities before purchase of components or integration in a lab environment. For these efforts the Contractor shall developed detailed designs, to include equipment lists or identification of required software for follow-on implementation. The Contractor shall develop detailed designs using the approved strategy or plans from prior phases. Under these services, the Contractor shall coordinate with Government personnel to transition or implement new capabilities. Performance of these services will be measured against ability to meet time (schedule) and labor (costs) proposed by the Contractor to accomplish efforts on a by-task basis. It is expected that this line of effort shall not have resources applied if there are no major services, modifications, or transitions tasked. It is also expected that *some level of* additional expertise to possibly include Consultants, OEM or OEM Certified Gold Partner

technical expertise, shall be provided as required in order to ensure appropriate expertise is assigned to these more complex tasks and that personnel performing day-to-day functions are not impacted accomplishing required task.

- IT Service Transition Services (Para 5.1.3 and associated subparagraphs). IT Service Transition Services consist of activities required to build out and demonstrate the capabilities before transitioning to operations. For these efforts the Contractor shall develop as built configuration packages, create new or modify *accreditation* packages, and create any documentation required to sustain a system from a maintenance perspective or to train Users. The Contractor shall implement the systems using the designs approved plans from prior phases. Under these services, the Contractor shall coordinate with Government personnel to transition or implement new capabilities. Performance of these services will be measured against ability to meet time (schedule) and labor (costs) proposed by the Contractor to accomplish efforts on a by-task basis. It is expected that this line of effort shall not have resources applied if there are no major services, modifications, or transitions tasked. It is also expected that *some level of* additional expertise, to possibly include OEM Consultants or OEM Certified Gold Partner technical expertise, shall be provided as required in order to ensure appropriate expertise is assigned to these more complex tasks and that personnel performing day-to-day functions are not impacted accomplishing required task.

- IT Service Operations Services (para 5.1.4, 5.1.5, 5.1.6 and associated sub paragraphs). IT Service Operations Services consist of activities required to sustain and protect all systems and ensure that Users and IT leadership are aware of the status of systems in order to assess any impacts to operations. This work also includes integration of life cycle replacement hardware, as well as, user applications, platform or infrastructure software. The Contractor shall ensure that all operations service functions incorporate documentation as a result of changes developed in prior phases. These efforts are repetitive in nature and as such the Contractor shall provide continuous periodic status updates and reports to Government personnel. Under these services, performance will be measured against ability to meet minimum performance requirements outlined in this PWS. The Contractor shall develop and report Key Performance Indicators that shall be used for situational awareness, planning, and IT Life Cycle or performance decision making. The Contractor provided IT Service Operations functions provided at all locations shall be common services delivered under the same standards, processes, and procedures unless specified otherwise. Some locations have additional unique and specifically outlined services.

- Continuous IT Service Improvement (para 5.1.7 and associate sub-paragraphs). IT Service Improvement activities enable modification to systems or processes to increase efficiency or effectiveness. The Contractor shall review current capabilities and processes and present changes if deemed beneficial. The Contractor is tasked to continuously review all processes and make efficiency recommendations that reduce costs or manpower, with no decrease in performance or increase performance at no additional costs. The Contractor

shall provide recommendations to the COR to address whether modifications to the contract are necessary. If no modification is required, the Contractor shall implement change as soon as possible after approval from the COR.

- Software Engineering and Integration/Application Life Cycle Support Activities (Para 5.1.9). SC has and requires unique applications or the adaptation of commercial-off-the-shell applications to accomplish its missions. The Contractor shall accomplish Software Engineering and Integration (SEI) activities to include adapting commercial off-the shelf systems or develop custom applications for implementation in local or cloud hosted environments. Performance of these services will be measured against ability to meet time (schedule) and labor (costs) proposed by the Contractor to accomplish efforts on a by-task basis. It is also expected that ***some level*** of Consultants, OEM or OEM Certified Gold Partner technical expertise shall be provided as required in order to ensure appropriate expertise is assigned to these more complex tasks when needed.

- IT Systems Support Services (Para 5.1.10 and associated subparagraphs). IT Systems Support Services entail background activities required to sustain the IT environments. There are three sub-classes of these Services. The first sub-class is IT Systems Operations and Maintenance Support Services which consists of those services required to enable daily operations of systems. For these Services, the Contractor shall provide project management, budgeting, procurement, logistics, information assurance, configuration management. The second sub-class are User Support Services. For these services, the Contractor shall support Users directly through training or adaptation of mission systems or web portals. Finally, the third-subclass is IT Systems OEM Support Services; under this area, the Contractor shall provide OEM support at the enterprise level or for specific systems.

- JTF-Bravo, JTF-GTMO, and Colombia Supplemental IT Support Functions (Par 5.1.11). JTF Bravo, JTF-GTMO, and Colombia have unique IT support requirements due to the complexity of on-going missions or the local environment. At JTF-Bravo, JTF-GTMO and Colombia, the Contractor shall provide specific support functions to augment the mission. These efforts are collaborative in nature and as such The Contractor may work side-by-side with Government personnel.

- Exercise and Contingency Operations Support Functions (Par 5.2.4). SC must be ready to support real world contingencies at any time. In preparation for contingencies, the Command executes periodic exercises at prescribed times during the year. In addition, mechanisms must be available to enable surge during real-world contingencies. The Contractor shall provide services to support exercises and contingencies. It is expected that this line of effort shall not have resources applied if there are no Exercises or Contingency Operations tasked.

5.1.1 Enterprise IT Service Strategy and Planning

The Contractor shall provide technical and programmatic support to assist SCJ6, 525th Signal Company, JTF-Bravo, and JTF-GTMO communicators with all aspects of IT service strategy related to development, planning, engineering, fielding and operating IT systems and resources. Based on Government requirements, the Contractor shall present recommendations to help decide on areas of change for IT and Service Management capabilities in support of the SC's overall strategic vision. Work in this area shall help the Government define and develop plans with regard to its services and the management of those services. The Contractor recommendations shall help determine which services are best suited to meet mission outcomes, as well as, the criteria to effectively manage and measure those services. At the direction of the Government, the Contractor shall add new services to the IT Service Catalog developed and maintained by the Contractor. In support of Service Strategy and Planning efforts, the Contractor shall provide high level concept presentations and/or concepts of operation, technical requirements in support of operational or functional requirements, as well as, support detailed reviews, analysis and coordination of processes, policy, doctrine, directives, regulations and implementation instructions. Assessments, strategies, technical requirements, plans, and policies shall address all aspects of life cycle support (system design, system transition, system operation) as appropriate.

5.1.1.1 Phase-In Plan for Assumption of Operations and Maintenance of USSOUTHCOM Communications Systems and Deprecation of TCSC, JTF-Bravo, and JTF-GTMO SIPRNET and NIPRNET Networks in the AOR.

The Contractor shall accomplish assessments and develop a Phase-In Plan for assuming responsibility for execution of operations and maintenance, as well as, all life-cycle support activities of all SC IT on a "by-location", "by-network" or by "effort", basis. The Contractor shall synchronize the plan to assume responsibilities in accordance with schedule for existing task order/contract completion identified in Attachment 1. The plan shall also address consolidation of functions and remote management of all IT environments from SC HQ, as well as, deprecating all SIPRNET and NIPRNET networks as soon as possible from existing and subsequent locations after assumption of responsibilities for each location/network. The SC HQ SIPRNET and NIPRNET networks will remain as the only networks for the entire AOR. The TCSC, JTF-Bravo and JTF-GTMO SIPRnet and NIPRnet shall be depreciated such that any required networks components at any locations services by these networks are extensions for the SC HQ networks. It is expected that the remote management and deprecation of networks will reduce or eliminate resources supporting the same or similar functions at different locations. The list of locations, contracts, and estimated task order completion dates is contained in Attachment 1. See attachment 26 for generic diagram of networks to be Deprecated. (Deliverable # 10, Attachment 1)

5.1.1.1.1 IT Service Corrective Action Planning

The Contractor shall assess the current configuration of all IT services at each location or effort identified in Attachment 1 to verify the components are installed/integrated in a manner that enables 99.85% availability for each respective service after TCSC, JTF-Bravo and JTF-GTMO SIPRNET and NIPRNET deprecation. The Contractor shall complete the assessment after assumption of operations and maintenance responsibilities at a given site. Attachment 9 contains a list of all IT services and systems by location. If the existing configuration does not support the respective service level after TCSC, JTF-Bravo and JTF-GTMO NIPRnet and NIPRnet deprecation, the Contractor shall identify and develop corrective action plans required to maintain respective services at 99.85% availability. Availability of IT services at 99.85% means that on a monthly basis, a given IT service is only unavailable to any user no more than 1 hour per month exclusive of approved scheduled outages and exclusive of external connectivity or other infrastructure factors. The 99.85% availability of a service also assumes that the network infrastructure (routers, switches, and personal computers, or telephone instruments) are also available. If changes are required to meet the 99.85% availability rate after TCSC, JTF-Bravo and JTF-GTMO NIPRnet and NIPRnet deprecation, the Contractor shall implement appropriate Service Design tasks (5.1.2.1.1) and subsequent processes. (Deliverables 3, 11, Attachment 1). Note that the Government reserves the right to update systems to meet availability requirements through other means and provide the solutions as GFE to the Contractor just as all the current systems are considered GFE.

5.1.1.2 Joint Information Environment (JIE) Transformation Planning

The Contractor shall accomplish assessments and develop high level plans, preliminary designs, as well as, associated policies and recommended changes to life-cycle operations and maintenance processes to accomplish the following JIE subtasks in the SC AOR. These tasks are generalized as *Technical Requirements Assessment and Planning Tasks* for all paragraph 5.1.1.2 subtasks. JIE planning is applicable to SIPRNET, NIPRNET, and SC managed MNIS at all locations. JIE planning is not applicable to special missions systems or programs of record. The Attachment 11 JIE technical guidelines are applicable to this effort and supersede any requirements identified in the following sub-tasks which may conflict. Attachment 11 contains the current state and future state of associated JIE migration tasks. (Deliverable # 13, Attachment 1)

5.1.1.2.1 Data Center Consolidation Planning

The Contractor shall accomplish *Technical Requirements Assessment and Planning Tasks* to consolidate and centrally manage all server farms in the SC AOR. The Contractor shall assess the current data center configurations and identify or re-identified and catalog all physical and virtual servers at each Installation Processing Node (IPN) or Installation Service Node (ISN). The Contractor shall catalog the purpose and exact software configuration of each physical and virtual server to include operating system, processor, memory, and storage allocations. The Contractor shall make recommendations to maintain the server functions (physical or virtual) at respective IPNs, move to the SC HQ IPN, or move to a Core Data Center. All storage (on the

server or on a storage area network) shall also be assessed and recommendations made to align storage with servers. The Contractor shall accomplish the transition in two Data Center Consolidation (DCC) phases. In DCC Phase 1, all Data Centers are configured as ISNs and only the SC HQ is an IPN providing applications hosting to the AOR and application replication to the SC DRSC site. Bandwidth permitting, the Contractor shall consider the SCO located data centers for conversion to Geographically Separated Units (GSUs) on a site-by-site basis. In DCC Phase 2, the Contractor shall convert SCHQ to an ISN with all applications operating at a DISA Core Data Center or a DoD approved Commercial Provider Data Center under either the Hosted Services or Platform as a Service constructs. The Contractor shall accomplish this task in conjunction with 5.1.1.2.2 Software as a Service Planning. The Contractor shall propose the timelines for each phase based on the level of effort required to accomplish tasks and factoring any required life-cycle-replacement actions at a given node. (Deliverable # 13, Attachment 1)

5.1.1.2.2 Software-as-a-Service Planning

The Contractor shall accomplish *Technical Requirements Assessment and Planning Tasks* for migration of all server-based and client-based user applications in parallel with data center consolidation efforts (paragraph 5.1.1.2.1) in the SC AOR. As part of this effort, the Contractor shall assess server and client applications for transition either to a DoD Enterprise Service, transition as a SC Hosted Theater Service, remain as a local service, be eliminated, or be upgraded to a newer version. The Contractor assessment shall also include a determination of which applications (i.e. and associated servers) shall not be routed outside of NIPRNET or SIPRNET. During DCC Phase 1, the Contractor shall assess applications at each IPN that are not DoD Enterprise Services, for migration to the SC HQ IPN and integrate them to operate with the SC Data Replication in Support of COOP (DRSC) site. In DCC Phase 2, the Contractor shall transition all applications at the SC HQ IPN not required to run an ISN or GSU to hosted services at a DISA Core Data Center or DoD approved Commercial Provider Data Center under the Hosted Services or Platform as a Service Constructs. (Deliverable # 13, Attachment 1)

5.1.1.2.3 Active Directory Planning.

The Contractor shall accomplish *Technical Requirements Assessment and Planning Tasks* to normalize all Active Directory Structure and Domain Name Service (DNS) at each SC IPN/ISN/GSU. This includes assessing which applications (i.e. and associated servers) are aligned to respective application portfolio/domain types and shall not be routed outside of NIPRNET or SIPRNET. The Contractor shall accomplish a parallel effort to create v-LANs to match each Active Directory structure. (Deliverable 13, Attachment 1)

5.1.1.2.4 Identity and Access Management (IdAM) Planning

The Contractor shall accomplish *Technical Requirements Assessment and Planning Tasks* to meet DoD IdAM requirements (http://iase.disa.mil/idam/idam_portfolio.html). The Contractor shall modify existing SC IdAM tools to integrate with external (non-SOUTHCOM) IdAM systems

such as Identity Synchronization Service (IdSS), Real-time Broker Service (RBS) and/or Batch-Broker Service (BBS). The Contractor provided IdAM capabilities shall allow any individual to automatically access common applications that do not require elevated rights based on Persona information. The Contractor provided IdAM capabilities shall include workflows and associated tools to enable members to request elevated rights to applications or to allow operational managers to automatically give elevated rights based on Persona. The Contractor accomplished planning assessment shall include a matrix that identifies how each recommendation or technical requirement to be implemented satisfies DoD IdAM requirements. (Deliverable # 13, Attachment 1)

5.1.1.2.5 Client Modernization (CM) Planning

The Contractor shall accomplish *Technical Requirements Assessment and Planning Tasks* to develop and implement Client Modernization at each major installation in the SC AOR. The Contractor shall factor the results of the Software-as-a-Service assessment (paragraph 5.1.1.2.2) in the Client Modernization Plan. The Contractor developed Client Modernization Plan shall include a technical architecture, as well as, life-cycle cost-benefit analysis for implementation of one or combinations of fat-client, zero-client, thin-client, or HTML-5 browser only clients. The Contractor's assessment shall also factor bandwidth and connectivity availability. (Deliverable # 13, Attachment 1)

5.1.1.2.6 SC Single Security Architecture Planning

The Contractor shall accomplish *Technical Requirements Assessment and Planning Tasks* to implement a Single Security Architecture (SSA) in the SC AOR. When developing the SSA, the Contractor shall factor the existing configuration of all Security Systems (i.e. Security Stacks) on each SC network, as well as, management of systems and reporting processes. The Contractor shall assess and make recommendations to standardize management, operational, and technical security controls of the proposed Single Security Architecture. (Deliverable # 13, Attachment 1)

5.1.1.2.7 Unified Capabilities Planning

The Contractor shall accomplish *Technical Requirements Assessment and Planning Tasks* to transition existing voice, data, video, and collaboration systems in accordance with Unified Capabilities Requirements guidelines (http://www.disa.mil/Services/Network-Services/UCCO/Policies-and-Procedures). The intent is to migrate all data, voice, video and collaboration services in the SC AOR to Everything Over IP (EOIP). (Deliverable # 13, Attachment 1)

5.1.1.3 New Communications Systems Capability Planning

The Contractor shall accomplish *Technical Requirements Assessment and Planning Tasks* to implement new systems or capabilities that meet future requirements. Capabilities may be in the form of process changes, applications, systems, software, hardware, or combinations thereof. The future assessments shall include a matrix identifying how each recommendation satisfies the proposed communications systems requirements. Assessments shall factor options for GOTS, COTS, or combinations thereof if applicable. The assessment shall also include a high level transition plan, and preliminary design, as well as, associated policies and recommended changes to life-cycle operations and maintenance processes to operationalize the system. (Deliverable # 14, Attachment 1)

5.1.1.3.1 New Requirements Impacts to Service Operations.

The Contractor shall review and support all incoming Information Technology Requests (ITR). The ITR process is the means for Users to request capabilities. The Contractor shall help the Government assess if the ITR can be satisfied within the existing services (I.e. is part of the existing service catalog) or whether the requirements shall be planned, designed, integrated and transitioned. (Deliverable # 14, Attachment 1)

5.1.1.3.2 Facility Site Analysis

If required for new Communications Systems Planning, the Contractor shall perform facility site analysis and site surveys. (Deliverable # 14, Attachment 1)

5.1.1.3.3 VSAT Site Survey and Installation Plan

Prior to the installation of new VSAT terminal equipment, The Contractor shall perform a site survey to determine look-angles, cabling run lengths, and antenna location. When performing site surveys, the Contractor assess and if required negotiate antenna location, cabling runs, interfaces to other networks, and other issues with building management personnel and end users at each site. The contractor shall maintain and update or create, installation drawings for all VSAT locations. Prior to each site installation, the Contractor shall provide the government with a copy of the site's Installation Plan. The Contractor shall ensure the plan contains a master schedule listing all milestones for completing the installation. (Deliverable # 33 Attachment 1)

5.1.1.3.3.1 VSAT Permissions

The Contractor shall work with the Government to obtain all permits, licenses, landing rights, custom duties, and host nation approvals (HNA) for the transmission of radio frequency signals within each country and province for all sites. The Contractor shall obtain permission from the proper authority to mount the VSAT antenna and its outdoor components on the roofs, or other locations on building grounds. The Contractor shall obtain permission from the COR to route power and cabling to the antenna on the roof or other location on the building grounds. The

Contractor shall identify all tariffs or building permits requirements and obtain approval prior to execution to ensure re-imbursement and identify these requirements in the Satellite installation plan. (Deliverable 33, Attachment 1)

5.1.2 Service Design

The Contractor shall provide technical and programmatic support to assist SCJ6, 525th Signal Company, JTF-Bravo, and JTF-GTMO communicators with all aspects of IT systems *Service Design*. Service Design ensures that services are designed to align and match current and future technical and operational requirements. For all subparagraphs, Service Design includes all the engineering services required to develop a *Service Design Package* which includes the following artifacts as appropriate: a) detailed architectures, b) drawings, c) equipment lists, d) process descriptions, e) policies and other appropriate documentation such as f) test plans, as well as, g) timelines, g) dependencies, h) assumptions, i) required manpower (by labor category and hours) in the transition and O&M phases, j) equipment, and k) circuits to meet current and future agreed mission requirements and associated life cycle sustainment efforts.

The Contractor shall accomplish Service Designs after applicable service paragraph 5.1.1 Assessments and Plans are approved.

5.1.2.1 Design for Deprecation all Non-SC HQ SIPRNET and NIPRNET Networks.

The Contractor shall develop a *Service Design Package* (SDP) to deprecate all SIPRNET and NIPRNET networks in the AOR in accordance guidance obtained from completion of task 5.1.1.1. The SDP shall contain all of the artifacts required to create single NIPRNET and SIPRNET instances in the AOR. (Deliverable # 89, Attachment 1)

5.1.2.1.1 IT Service Corrective Action Service Design

The Contractor shall develop a *Service Design Package* (SDP) to address corrective actions approved by the Government as a result of IT Service Corrective Action Assessments (para 5.1.1.). The SDP shall contain all of the artifacts required to provide the IT Service at 99.85% availability after SIPRnet and NIPRnet deprecation. (Deliverable # 16, Attachment 1)

5.1.2.2 Joint Information Environment Design

The Contractor shall accomplish Service Design and develop the *Service Design Packages* to accomplish the following JIE design subtasks in the SC AOR. (Deliverable # 17, Attachment 1)

5.1.2.2.1 Data Center Consolidation Design

The Contractor shall develop the *Service Design Packages* to centrally manage all server farms in the SC AOR in accordance with approved recommendations, designs, and guidance obtained

from completion of task 5.1.1.2.1. This task is accomplished in conjunction with 5.1.2.2.2 Software-as-a-Service Design. (Deliverable # 17, Attachment 1)

5.1.2.2.2 Software as a Service (SaaS) Design

The Contractor shall develop the *Service Design Packages* to implement the approved technical requirements identified Software as a Service technical requirements planning tasks (i.e. paragraph 5.1.1.2.2) (Deliverable # 17, Attachment 1)

5.1.2.2.3 Active Directory Design

The Contractor shall develop the *Service Design Packages* to implement the approved technical requirements identified in the Active Directory requirements planning tasks (i.e. para 5.1.1.2.3). (Deliverable # 17, Attachment 1)

5.1.2.2.4 Identity and Access Management (IdAM) Service Design

The Contractor shall develop the *Service Design Packages* to implement approved technical requirements identified in the IdAM requirements planning task (i.e. paragraph 5.1.1.2.4). (Deliverable # 17, Attachment 1)

5.1.2.2.5 Client Modernization Design

The Contractor shall develop the *Service Design Packages* to implement approved technical requirements identified in the Client Modernization requirements planning task (i.e. paragraph 5.1.1.2.5). (Deliverable #17, Attachment 1)

5.1.2.2.6 SC Single Security Architecture (SSA) Design

The Contractor shall develop the *Service Design Packages* to implement approved technical requirements identified in the SSA requirements planning task (i.e. paragraph 5.1.1.2.6). (Deliverable #17, Attachment 1)

5.1.2.2.7 Unified Capabilities Design

The Contractor shall develop the *Service Design Packages* to implement approved technical requirements identified in the Unified Capabilities (UC) requirements planning task (i.e. paragraph 5.1.1.3). (Deliverable #17, Attachment 1)

5.1.2.3 New Communications Systems Capability Design

The Contractor shall develop the *Service Design Packages* to implement new capabilities or services after completion of the corresponding paragraph 5.1.1.3 planning task. (Deliverable, # 18 Attachment 1)

5.1.2.4 Cybersecurity In the Service Design Phase

The Contractor shall start accreditation documentation and make necessary changes/additions to the SC Risk Management Framework (RMF) packages during the design phase for any new or modified service or system. (Deliverable #18, Attachment 1)

5.1.3 IT Service Transition

The Contractor shall provide technical and programmatic support to assist SCJ6, 525th Signal Company, JTF-Bravo, and JTF-GTMO communicators with all aspects of communications/computer systems service transition. In order to ensure new capabilities are ready for operation, the Contractor shall accomplish the following *IT Service Transition Activities* for all new IT Service Designs or IT system redesigns: a) transition planning and support to include verification that Operations and Maintenance personnel are properly trained to manage all required system components, b) integration of equipment, systems or services in a manner that meets appropriate Service Design, c) release and deployment management, d) service validation and testing, e) evaluation, f) submission of test reports, g) submission of as-built drawings, installation plans, interface control documents for data, power and cooling, and facility interface drawings, h) submission of operations and maintenance instructions, and i) release of user training plans and materials. Service Transition activities apply for all subparagraphs. In support of Service Transition the Contractor shall provide Engineering Services and maintain and Engineering Lab.

a. Engineering Services in support of the Service Transition. The Contractor shall prototype, document, and accomplish acceptance testing on all new capabilities or modifications. Acceptance testing shall include Functional Configuration Verifications and Audits; the contractor shall verify the system and subsystem configuration documentation complies with their functional performance characteristics before acceptance into an architectural baseline. (Deliverable # 61 Attachment 1)

b. Engineering Lab. The Contractor shall operate, maintain, and use the SOUTHCOM LAN test-bed configuration for the purpose of Contractor evaluation of upgrades to SOUTHCOM IT assets proposed through either life-cycle upgrades or via the Information Technology Request process. The Contractor shall also utilize the SC test-bed for system troubleshooting and problem resolution for all SC users. Additionally, the Contractor shall use the engineering lab LAN to test software version upgrades and to develop manuals and training material. The Contractor shall not transition changes to the operational environment without prior successful

testing and ACOR approval. The Contractor shall request guidance and accomplish software testing related to patches, STIGS, and IAVAs, on a case-by-case basis if it is perceived that the change will impact availability of any operational service.

In addition to the above, in accomplishing service transitions, the Contractor shall also factor the following Cybersecurity Service Transition Associated Tasks if required.

a. Change Management. The Contractor shall integrate Information Assurance (IA) and security principles in the Change Management process in the design and development phase.

b. Certification and Accreditation (C&A) Packages. The Contractor shall develop and maintain C&A documentations (including Program of Record (POR) and Program Managed Systems) for SIPRNet, Coalition, and NIPRNet connection approval processes. This includes network diagrams, IP ranges, COOP and disaster recovery plans, and the number of systems by type. Ensure C&A documentation is populated and maintained in the appropriate SIPRNET or NIPRNET Enterprise Mission Assurance Support System (eMASS).

c. Ports and Protocol. The Contractor shall comply with DoD ports and protocol management program to include tracking and documenting approved "opened" ports and protocols.

5.1.3.1 Deprecation of SIPRNET and NIPRNET Networks - Service Transition.

The Contractor shall accomplish Service Transition activities to deprecate all SIPRNET and NIPRNET networks in the AOR. The Contractor shall implement the network deprecation transition in accordance with approved design obtained from completion of task 5.1.2.1. (Deliverable 90, Attachment 1)

5.1.3.1.1 IT System Corrective Action Service Transition

The Contractor shall accomplish the IT Service Corrective Action Service Transition approved by the Government as a result of IT Service Corrective Action Service Design (para 5.1.2.). (Deliverable # 19, Attachment 1)

5.1.3.2 Joint Information Environment Transition

The Contractor shall accomplish Service Transition activities for the following JIE efforts. (Deliverable # 20 Attachment 1)

5.1.3.2.1 Data Center Consolidation Transition

The Contractor shall accomplish Service Transition activities for Data Center Consolidation efforts. The Contractor shall accomplish this task in conjunction with 5.1.3.2.2 Software as a Service Transition. The Contractor shall implement the transition in accordance with approved design obtained from completion of task 5.1.2.2.1. (Deliverable #20, Attachment 1)

5.1.3.2.2 Software-as-a-Service Transition

The Contractor shall accomplish Service Transition activities for Software-as-a-Service efforts. The Contractor shall accomplish this task in conjunction with Data Center Consolidation Transition. The Contractor shall implement the transition in accordance with approved design obtained from completion of task 5.1.2.2.2. (Deliverable # 20 Attachment 1)

5.1.3.2.3 Active Directory Transition

The Contractor shall accomplish Service Transition activities for Active Directory at each SC IPN, ISN or GSU . The Contractor shall implement the transition in accordance with approved design obtained from completion of task 5.1.2.2.3. (Deliverable # 20 Attachment 1)

5.1.3.2.4 Identity and Access Management (IdAM) Transition

The Contractor shall accomplish Service Transition activities for IdAM efforts. The Contractor shall implement the transition in accordance with approved design obtained from completion of task 5.1.2.2.4. (Deliverable # 20 Attachment 1)

5.1.3.2.5 Client Modernization (CM) Transition

The Contractor shall accomplish Service Transition activities for CM efforts. The Contractor shall implement the transition in accordance with approved design obtained from completion of task 5.1.2.2.5. (Deliverable # 20 Attachment 1)

5.1.3.2.6 SC Single Security Architecture Transition

The Contractor shall accomplish Service Transition for SSA efforts. The Contractor shall implement the transition in accordance with approved design obtained from completion of task 5.1.2.2.6. (Deliverable # 20 Attachment 1)

5.1.3.2.7 Unified Capabilities Transition

The Contractor shall accomplish Service Transition for Unified Capability efforts. The Contractor shall implement the transition in accordance with approved design obtained from completion of task 5.1.2.3. (Deliverable # 20 Attachment 1)

5.1.3.3 New Communications Systems Capability Transition

The Contractor shall accomplish Transition efforts to implement a future US or multinational Communication Systems capabilities. The Contractor shall implement the transition in accordance with approved design obtained from completion of the corresponding 5.1.2.4 task. (Deliverable # 21 Attachment 1)

5.1.4 Service Operations

The Contractor shall accomplish Service Operations for all IT systems and services; unless specific by the COR, these services are only applicable for systems installed or operated at SC HQ, JTF-Bravo, JTF-GTMO and the SCOs. The Contractor shall ensure the continuous availability of all SC IT services at a 99.85% rate exclusive of approved service outages, man-made, or natural disasters. Specific Service Operations elements include not only ensuring the IT systems and services are available but also that all major subsystems (Servers, Storage Area Networks, Networking/Communications Systems, VTC Systems, and Telephone Systems) are maintained in accordance with Original Equipment Manufacturer (OEM) best practices. Service Operations also includes integration of life cycle replacement of hardware, as well as, user applications, platform or infrastructure software. The Contractor shall adhere to OEM best practices to include implementing periodic updates, DISA Security Technical Information Guidance (STIG) and CYBERCOM orders, directives, and Information Assurance Vulnerability Management (IAVM) notices in coordination with the ACOR. STIG guidance and IAVM notice implementation shall supersede OEM best practices. The Contractor shall inform the Government if STIG and IAVM mandated changes affect service availability or capabilities. The Contractor shall coordinate and synchronize the following sub-tasks and activities with respective communications ACOR leads at each location. (Deliverable # 22, 23,24, Attachment 1)

5.1.4.1 Service Operations and Maintenance Plan

The Contractor shall develop and maintain an overall Operations and Maintenance Plan that addresses and synchronizes all the activities of paragraph 5.1.4 and associated sub-paragraphs. The Contractor shall outline in the Operations and Maintenance Plan all the processes to be executed, which work centers (e.g., Tier 1, Tier 2, System Administration, etc.) shall be involved, and identify specific technical personnel to include duty titles, skill sets, certifications, and experience required to accomplish the various aspects of accomplishing Service Operations and Maintenance.

The Service Operations and Maintenance Plan shall include a table of periodic processes to be accomplished and when the deliverables or status from those processes are due. The Service Operations and Maintenance Plan shall identify relationships to IT Support Services such as OEM Support, Training, Configuration Management, Logistics, Procurement, TNCC Support,

Technical Control Facility operations, and DoDIN service connectivity. The Operations and Maintenance Plan shall also factor life-cycle support activities such as establishing and maintaining a spares pool for all critical equipment, replacing critical components of critical equipment, life cycle replacement of all major components, and discussion on which maintenance processes shall out be outsourced to Consultants, OEM Certified Partners, OEM or local vendors. The Contractor shall identify systems that require OEM or OEM certified gold partner verification of configuration on a periodic basis. The Contractor shall also identify systems that require OEM certification for operations and maintenance personnel. The Government may direct specific OEM certifications for any system component if the Contractor does not identify the requirement during the development of the Service Operations and Maintenance Plan.

The Service Operations and Maintenance Plan shall contain an attachment identifying when all Hardware, as well as, User applications and infrastructure or platform software will be life cycled. This attachment will be synchronized with the Life Cycle Procurement Plan.

The Contractor shall repair all IT systems components in accordance with the approved Operations and Maintenance Plan. The Contractor shall ensure the Operations and Maintenance Plan factors the following:

a) Requirements for all workstations or peripherals such as monitors or printers, to be repaired within 72 hours of report of outage. The Contractor shall install temporary (floating) workstations and peripherals from the spares pool while workstations and peripherals are being repaired. The Contractor shall accomplish all workstation and peripheral repairs using Best Commercial Practice guidelines.
b) Documentation of repairs in a maintenance log and include the documentation in the monthly status report. The Contractor shall verify and report all unserviceable equipment beyond economically repairable to the appropriate ACOR for disposition.
c) Government relief for un-manned site repair actions. For equipment at remote or un-manned sites (in accordance with Attachment 6), the COR has the authority to delay after hour repairs until the next business day or longer if travel approval is required. In cases of an outage or serious impairment to a Service or System at remote locations, the Contractor shall dispatch personnel within 90 minutes after travel approval in the most direct and safest manner. For the purposes of this PWS, remote sites (locations) are defined as any location without on-site support.
d) The process to coordinate for Authorized Service Interruptions required to perform maintenance actions.

(Deliverable # 22 Attachment 1)

5.1.4.2 Service Desk Services/Tier 1 Service

The Contractor shall assume responsibility of Help Desk functions at each location on an as-is basis. The Contractor shall develop and execute a plan to transition the independent Help Desks to a single AOR wide Service Desk Function. The Contractor shall act as the single central point of contact for all users of IT in the AOR and shall log and manage all incidents, service requests and access requests. The Contractor shall provide Service Desk representatives at JTF-Bravo, JTF-GTMO, and permanently manned SCOs with the maximum number of Service Desk Representatives at the SC HQ facility. The Contractor shall transition the Service Desk functions from the JTF-Bravo, JTF-GTMO and SCOs with On-Site Support to the HQ SC facilities after normal duty hours specified for each location. The Government may augment the Service Desk with Government personnel; under this case, the Contractor shall assume responsibility of the assigned tasks after verification of the work orders.

5.1.4.2.1 Incident and Service Request Ticketing System

The Contractor shall transition independent incident and service request systems at each location to a single Incident and service request ticketing system for the AOR. The Contractor shall keep the service request system current with a catalog of all available services and systems in the AOR. The Contractor shall work with the appropriate ACOR to determine the service request system that shall be used throughout the AOR. For planning purposes, the Contractor shall plan on migrating to the Service Now platform.

5.1.4.2.2 Service Desk User Collaboration Tools

The Contractor shall implement and operate real-time chat tools to help Users address incidents and service requests in addition to manning telephone lines. The service desks shall also receive service requests or incidents by customer walk-ins at each location.

5.1.4.2.2.1 Frequently Asked Questions

The Contractor shall analyze the service desk/ticket database and shall make recommendations to reduce the number of future service requests by responding to key problems, e.g., refining user training, developing online help screens, and publishing Frequently Asked Questions (FAQs) on the SC Portal or Service Management tool.

5.1.4.2.3 Initial Response to Incidents

The Contractor shall perform the assessments, and if applicable utilize remote access to User equipment or other devices to address incidents. The Contractor shall attempt to troubleshoot, isolate and resolve, or refer to the next level of Service.

5.1.4.2.4 User Application or IT Tools Support

The Contractor shall be proficient on all SC AOR applications and IT tools and provide customers with direct support on use of tools or be able to direct them to other personnel with detailed knowledge. The Contractor may re-direct questions to appropriate Contractor training or User support personnel or other Contractor subject matter experts based on level of difficulty.

5.1.4.2.5 Very Important Person (VIP) and Joint Operations Center and Crises Action Center Support

Joint Operations Centers are enduring Government work centers that maintain situational awareness of activities for the domain under their purview. Crises Action Centers are temporary Government work centers that augment Joint Operations Centers during exercises or real-world contingencies.

The Contractor shall provide immediate service to all General Officers (GO), Senior Service Executives (SES's) or other agency equivalents, SCO Commanders, JTF-Commanders, as well as, the Joint Operations Centers or Crises Action Centers at any locations. The Contractor shall handle Service Requests or Incident Reports for GO's and SES's at the highest priority, providing resolution plan within the technically allowable timeframe based on location. The Contractor shall coordinate resolution time and establish realistic timeframes for resolution of these work orders. The Service Desk shall maintain an ACOR approved list of all VIPs and Joint or Crises Operations Centers.

5.1.4.2.6 Prioritized Incident Management Process

The Contractor shall assess, make recommendations, and then implement a tiered priority incident management process. The Contractor shall raise any Priority ONE (P-1) incident that presents a technical or resource issue the local ACORs for de-confliction or the COR if required. The Contractor shall handle important incidents as Priority TWO (P-2). The Contractor shall assign Priority THREE (P-3) as the default to all other incidents. The following is the required priority incident scheme and criteria. Critical: Priority 1 = Immediate response (24x7); Urgent: Priority 2 = (4 hrs); Routine: Priority 3 = (24 – 72 hrs depending on device).

5.1.4.2.7 Customer Portable Asset Tracking and Control

The Contractor shall receive and distribute customer equipment such as PDAs, laptops, and cell phones utilizing form DA Form 2407 Maintenance Request. The Contractor is responsible for safeguarding all assets turned in to the Service Desks for maintenance or during customer personnel turnover. Contractor shall establish and maintain an Asset Management Database (AMD) to document all equipment turned in or provisioned to customers. (Deliverable # 25 Attachment 1)

5.1.4.2.8 Customer Service Desk Visitor Database Maintenance and Support

Contractor shall maintain a database of transactions of assets, visitors and issues handled at the Service Desks. This tool may be integrated with the Incident and Service Request system. The Contractor shall make data on all transactions available for viewing via a web based reports.

5.1.4.2.9 Security Cooperation Office (SCO) Tier 1 Support

The Contractor shall provide on-site support at the SCOs identified in Attachment 6. The term used by the SCOs for OCONUS on-site support is On-Site Technical Representative (OSTR). OSTRs shall act as Tier 1 Support in coordination with the Service Desk.

5.1.4.2.9.1 OCONUS OSTR Sponsorship

The OCONUS contractor personnel assigned to a Diplomatic or Consular missions are responsible for maintaining the day-to-day operational effectiveness of the USSOUTHCOM C4S architecture. On-site contractor personnel are tenants of the embassy, and are sponsored by the SCO Commander. The contactor shall deploy personnel for assignment status, i.e., contractor equivalent of Temporary Duty (TDY). The Contractor shall fully comply with all rules, procedures, and practices as required concerning the flow of information to or from the embassy and forward locations that come within the Ambassador/Chief of Mission's jurisdiction. Additionally, the Ambassador/Chief of Mission has control over the commercial firm's individual employees (non-personal services contractors) (and its subcontractors individual employees, where relevant), including in particular a right of withdrawal from the host country of individual personnel. The government will include the OCONUS contractors in the SCO's International Cooperative Administrative Support Services (ICASS) System agreement 2122-1 for Basic Service cost Center 6150 contractor eligible support items negotiated between the DOD and the DOS.

The contractor shall ensure the following before contrator personnel depart from the United States or a third country, and before contractor personnel residing in the host country begin contract performance in the designated operational area or supportintg the diplomatic or consular mission:

a. All required security and background checks are complete and acceptable IAW PWS Paragraph(s) 1.6.22.

b. All personnel are medically and physically fit and have received all required vaccinations IAW PWS Paragraph(s) 4.1.

c. All personnel have all necessary passports, visas, entry permits, and other documents required for Contractor personnel to enter and exit the foreign country, including those required for in-transit countries IAW PWS Paragraph(s) 1.6.13.1.

d. All personnel have received -

1. A country clearance and special area clearance, if required by the chief of mission; Country clearance requests shall be submitted utilizing the Aircraft and Personnel Automated Clearance System at https://apacs.dtic.mil/apacs

2. Theater clearance, if required by the Geographic Combatant Commander.

3. All personnel have received personal security training. The training must at a minimum cover safety and security issues facing employees overseas.

4. All personnel have received isolated personnel training, if specified in the contract. Isolated personnel are military or civilian personnel separated from their unit or organization in an environment requiring them to survive, evade, or escape while awaiting rescue or recovery.

5. All personnel who are US citizens are registered with the U.S. Embassy or Consulate with jurisdiction over the area of operations at http://www.travel.state.gov

e. The contractor shall notify all personnel who are not a host country national or ordinary resident in the country that:

1. If this contract is with the Department of Defense, or the contract relates to supporting the mission of the Department of Defense outside the United States, such employees, and dependents residing with such employees, who engage in conduct outside the United States that would constitute an offense punishable by imprisonment for more than one year if the conduct had been engaged in within the special maritime and territorial jurisdiction of the United States, may potentially be subject to the criminal jurisdiction of the United States (see the Military. Extraterritorial Jurisdiction Act of 2000 (18 U.S.C. 3261 et seq.)
2. Pursuant to the War Crimes Act. 18 U.S.C. 2441, Federal criminal jurisdiction also extends to conduct that is determined to constitute a war crime when committed by a civilian national of the United States.
3. Other laws may provide for prosecution of U.S. nationals who commit offenses on the premises of United States diplomatic, consular, military or other United States Government missions outside the United States (18 U.S.C. 7(9)).

5.1.4.2.10 Service and Network Monitoring

The Contractor shall monitor appropriate systems for any degradation or outage and notify the appropriate ACOR at each SC HQ, JTF-Bravo, and JTF-GTMO, as well as, SC HQ Theater Network Coordination Center (TNCC). From a User perspective, services and systems include, all telephone/voice, video, collaboration systems, as well as, all key applications such as web portals, and web based or client-server based mission or administrative applications on SIPR and NIPR. From hardware/software perspectives, systems include application servers, network devices, and firewalls. (See Attachment # 12) for list of services and systems.

5.1.4.2.11 Service Catalog

The Contractor shall develop and maintain and IT Service Catalog outlining all services available to Users, as well as, services used to operate and protect the network. The Service catalog managed by the Contractor shall contain all services available throughout the SOUTHCOM AOR to include those maintained by the Contractor, Hosted by the Contractor, Hoteled by the Contractor as well as DoD Enterprise Services such as Enterprise Email, Defense Enterprise Portal, Defense Collaborative Tools, and Messaging. The Contractor shall add new Enterprise Services as they become available throughout the DoD.

The Contractor shall create processes and procedures to provision all SOUTHCOM users with any Service in the Service Catalog. The Contractor shall route requests for Services that are outside of the control of the Contractor to appropriate Service owners.

(Deliverable # 23, Attachment 1)

5.1.4.3 Tier 2 Technical Support

The Contractor shall provide Tier 2 support personnel to maintain all end user hardware to include personal computers, Virtual Desktop Infrastructure (VDI) devices, printers, faxes (commercial and secure), telephones (all variants), cell phones, laptops, PDAs. This includes corrective action to fix devices, complete or partial life-cycling of equipment, or returning to vendors for corrective action. The Contractor shall turn in equipment that is removed from use using appropriate documentation; the Contractor shall track the changes in appropriate configuration management and property book databases.

5.1.4.3.1 Desktop Integration and Testing

The Contractor shall provide integration, standardization, testing, evaluation, configuration control, and administration of desktop applications and peripherals.

5.1.4.3.2 Personal Computer Operating Systems and Applications

The Contractor shall remotely install standard baselines for operating systems, applications, and patches to all network connected personal computers using approved processes, procedures and tools. Contractor loading of applications directly on network connected personal computers via CD ROM or other local device, shall be on a case-by-case basis.

5.1.4.3.1.1 Desktop Baseline Permutations

The Contractor shall maintain permutations of the standard baselines for varying customer groups on a by-network basis. The Contractor shall evaluate existing permutations and revalidate their use. The Contractor shall keep track of which computers have which baselines

installed. The Contractor shall re-assess the number and configuration of desktop permutations as part of Software-as-a-Service implementation.

5.1.4.3.2 New Device Installation and Integration

The Contractor shall install, and integrate new client-level hardware to include but not limited to printers, multifunction printers, scanners, media devices, and personal digital assistant (PDAs) as part of normal life-cycle replacements or upgrades.

5.1.4.3.3 Hardware Repair

The Contractor shall repair or replace hardware at the Line Replaceable Unit (LRU) level. If a problem cannot be resolved at this level the Contractor shall escalate the issue to the next level. The Contractor shall provide recommendations to the COR on repair versus replacement actions.

5.1.4.3.4 Data-at-Rest

Contractors shall install and configure Data-at-Rest tools on laptops and PDAs as required in accordance with OEM specifications, STIG or CYBERCOM orders, directives and IAVM notices.

5.1.4.4 Tier 3 Support

The Contractor shall provide the following Tier 3 Support:

5.1.4.4.1 Server Farm Systems Administration

For purposes of this effort, Server Farms shall include physical and virtual servers or server or application appliances, applications on servers, and associated storage area networks (SANs). A list of servers and applications on servers by network, by location is contained in attachment 17. The Contractor shall accomplish the following Server Farm service operations functions:

5.1.4.4.1.1 System Administration

The Contractor shall provide system administration services for all servers, storage area networks (SANs), and server hosted applications on a by-network, by-location basis in accordance with the phase-in plan developed in paragraph 5.1.1.1. The Contractor shall provide Active Directory management and monitoring. Prior to implementing the Active Directory Normalization requirements (para 5.1.1.2.3, 5.1.2.2.3, and 5.1.3.2.3) the Contractor shall develop and execute means to remotely manage all servers under this task order, which is expected to reduce or eliminate resources supporting System Administration functions at appropriate locations. The Contractor shall ensure that implementation of Active Directory

Normalization and Data Center Consolidation Requirements shall factor means to centrally manage all the servers, SANs, and server hosted applications in the AOR. The Contractor shall develop a plan to re-align system administrators as part of the work related to paragraph 5.1.1.1.

5.1.4.4.1.2 User Access

The Contractor shall control and monitor user access to the User Devices, Servers, Applications, and Storage Area Networks. The Contractor shall add, delete, and modify user access to the network resources, manage account profiles, permissions, and access to resources, and create accounts within 24 hours of account request submission. The Contractor shall monitor, disable, and remove inactive accounts, as well as, control permissions. The contractor shall integrate and ensure common processes are accomplished at each location for providing User Access. The Contractor shall accomplish User Access functions by automated tools to the maximum extent possible. The Contractor shall transition all locations to use common Identity Access Management system and process as part of the paragraph 5.1.1.2.4. The Contractor shall maintain logs of all User Access changes that can be inspected on a no notice basis or used to generate electronic reports.

5.1.4.4.1.2.1 Verification of User eligibility for Access

The Contractor shall verify either through automated tools or with appropriate agencies that all users meet the requisite favorable security investigations, clearances, authorization, need-to-know, and security responsibilities before granting access to the C4 Systems. The Contractor shall ensure personnel are notified to accomplish system-specific and annual IA/CND awareness training through manual or automated means. User eligibility functions may be accomplished by automated tools or manual means. The Contractor shall transition all User eligibility functions to automated means at all locations as part of the Identity and Access Management System transition in paragraph 5.1.1.2.4.

5.1.4.4.1.3 Scripting Management

The Contractor shall automate repetitive system administration or network management processes to ensure efficiencies and effective handling of tasks. The Contractor shall implement COTS applications as applicable or develop scripts as required to support this effort. Examples of scripting tasks include the automation of the account creation process, renaming of a wide range of accounts to new naming conventions, and automatic notification to users on account statuses based on User roles or User database attributes. The Contractor shall modify/change/adjust scripts based on changes mandated by DOD guidance, SC J6 directives, upgrades, technical migrations, or organizational changes. The Contractor shall develop and maintain descriptions of all scripts. An example of one script is found in Attachment 26. (Deliverable # 26, Attachment 1)

5.1.4.4.2 Database Management and Administration

The Contractor shall function as the manager and administrator of databases on the SC enclaves. The Contractor shall provide database management and administration on a by-network, by-location basis in accordance with the phase-in plan developed in paragraph 5.1.1.1. The Contractor shall develop and implement means to remotely manage all databases in accordance with the Data Center Consolidation and Software-as-a-Service migration efforts under this Task Order, which is expected to reduce or eliminate resources supporting database management and administration functions at appropriate locations. The Contractor shall perform the following minimum functions in database environments:

5.1.4.4.2.1 Operate, Maintain, and Modify Databases

The Contractor shall maintain the existing common-user databases and design, structure, and maintain additional databases as required supporting new applications in accordance with OEM manufacturer, STIG, and CYBERCOM orders, directives and IAVM notices.

5.1.4.4.2.2 Database Analysis, Maintenance, and Corrective Action

The Contractor shall perform log analysis, error detection, fault correction, backups, and restores as required in accordance with OEM specifications, STIGS, or CYBERCOM Task Orders.

5.1.4.4.3 Theater Information Assurance Security Stack Maintenance

The Contractor shall maintain cybersecurity tools systems (i.e. firewalls, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), Vulnerability Scanning systems, Security Information Management system, Host Based Security Systems (HBSS), Content Filtering, Correlation Systems, Malware protection systems, application and device control systems) residing on SC networks. The Contractor shall ensure all changes to network security devices (e.g. firewalls, IDSs, IPSs, sensors, and HBSS, etc.) are submitted to and approved by the ACOR.

5.1.4.4.3.1 Antivirus Update Support

The Contractor shall support antivirus software updates. The Contractor shall manage the antivirus software by monitoring the United States Computer Emergency Readiness Team (US CERT) Web site (https://www.us-cert.gov/) at least twice a day for newly released definition updates and applying the definitions to the network servers and workstations.

5.1.4.4.4 Network Management Support

The Contractor shall operate, maintain, and assist the Government in life-cycle support all switches and routers and other network infrastructure equipment used on data, voice, and video networks. The Contractor shall provide network management support on a by network, by-location basis in accordance with the phase-in plan developed in paragraph 5.1.1.1. The Contractor shall maintain network equipment in accordance with OEM, STIG, and CYBERCOM orders, directives and IAVM notices. The Contractor shall and propose implement life cycle upgrades to network components in accordance with paragraph 5.1.1.3.Unified Capabilities Planning.

5.1.4.4.4.1 Network IP Range Management

The Contractor shall manage all wide area network IP ranges. The Contractor shall act as the SPIAN, SIPRNET, and NIPRNET Network Information Center's (NIC) technical POC for the southcom.mil and southcom.smil.mil domains. The Contractor shall coordinate with network managers and the SIPRNET and NIPRNET to maintain and update the DoD NIC web site on all domain or IP issues (NIC web site URL is: https://nic.mil/).

5.1.4.4.5 Domain Name Service (DNS) Support

The Contractor shall provide Primary and Secondary Domain Name Service (DNS) support for SC networks. The Contractor shall make recommendations to configure and name DNS sub-domains. The Contractor shall assist the Government in coordinating with DISA, where applicable, for DNS services.

5.1.4.4.5.1 DNS Support to Hoteled Systems

The Contractor shall provide Primary and Secondary DNS support for systems Hoteled on SC networks. The Contractor shall maintain a database of all Hoteled systems to include the name of systems, classification level, technical points of contact, program manager and associated point of contact. The Contractor shall ensure that all User requests for support for Hoteled systems are routed to the technical points of contact. See attachment 10 for a preliminary list of Hoteled systems. (Deliverable # 27, Attachment 1)

5.1.4.4.6 VPN Access and Gateways Support

The Contractor shall manage, operate, and support the secure and non-secure Virtual Private Network (VPN) access and gateways on SIPRNET, NIPRNET, as well as, specified multinational information sharing networks such as Partner Nations Network (PNN). The Contractor shall support user-access requirements.

5.1.4.4.7 Hoteled Systems Installation Support

The Contractor shall support connectivity of future Hoteled Systems to the networks and assist with troubleshooting connectivity problems as requested.

5.1.4.4.8 Data Replication in Support of Continuity of Operations (COOP) (DRSC) Operations and Maintenance

The Contractor shall remotely operate and maintain the DRSC site located in San Antonio, Texas. Travel may be required to resolve technical issues or to support back-up and restore processes.

5.1.4.4.9 Voice System Operations and Maintenance

The Contractor shall operate, maintain, and life cycle all secure and non-secure voice networks consisting of user telephone instruments to include plain telephone systems, Secure Telephone Equipment (STE) instruments, Sectera Viper instruments, and voice-over-IP (VoIP) network instruments.

5.1.4.4.9.1 Telecommunications Company (Telco) Telephone Line and Circuit Management

The Contractor shall manage the telephones lines Terrestrial Circuits provided by local telecommunications providers at each location. This includes appropriate Switching Units (Main or Remote Switching Units) or appropriate circuit transmission system at each location.

5.1.4.4.9.2 Voice Over IP Systems

The Contractor shall operate, maintain, program, and life-cycle all IP voice and video call processing, voice mail, contact center, emergency response, and integrated computing systems.

5.1.4.4.9.3 Telephone System Information Directory

The Contractor shall publish a web-based telephone directory for all telephone systems to include telephone dialing instructions, telephone use policies, and telephone numbers of all personnel with office symbols and duty titles. The Contactor shall implement automated tools and databases to accomplish this effort. (Deliverable # 28, Attachment 1)

5.1.4.4.16 IT System Usage Logs **(NOTE THE PARAGRAPH WILL BE MOVED AFTER AWARD)**

When tasked by the COR/ACOR, the Contractor shall produce usage reports for any system at any location. The report may be in any format that addresses the questions. (Deliverable # 29, Attachment 1)

5.1.4.4.10 Technical Control Facility /Network Operations Centers/Remote Hub Node Facilities or Data Centers

The Contractor shall support installation, testing, operations and maintenance of all circuit management systems (matrix switches, multiplexors, ATM switches) and associated equipment such as fiber optic models, channel service units, data service units at Technical Control Facility /Network Operations Centers/Remote Hub Node Faculties or Data Centers. The Contractor shall provide Technical Control Facility /Network Operations Centers/Remote Hub Nodes or Data Centers support on a by-location basis in accordance with the phase-in plan developed in paragraph 5.1.1.1. The Contractor shall develop and implement means to remotely manage all Technical Control Facility /Network Operations Centers/Remote Hub Nodes or Data Centers under this Task Order, which is expected to reduce or eliminate resources supporting Technical control/Network Operation Center/Remote Hub Node or Data Center functions at appropriate locations. The Contractor shall use OEM recommended/required, Government-Owned-Contractor-Operated testing equipment in support of the Tech Control Facility (TCF)/Network Operations Centers/Remote Hub Node or Data Center duties. The Government may augment any Technical Control Facility/Network Operations Center Remote Hub Node or Data Center with Government personnel; under this case, the Contractor shall assume responsibility of the assigned tasks after verification of the work orders or service outages.

5.1.4.4.10.1 COMSEC Equipment Operations and Maintenance

The Contractor shall receive, operate, trouble shoot, test and ship hand-receipt communications security (COMSEC) keying material, and associated key transfer devices, as well as, install digital and analog Controlled Cryptographic Items (CCI) and communications-electronic equipment. All shipping is on a cost–reimbursable basis and must be approved by the ACOR in advance. The Contractor shall maintain a list of all COMSEC and CCI identifying where the equipment is currently located and the hand-receipt holders. (Deliverable # 30, Attachment 1)

5.1.4.4.10.2 DISA Node Site Coordinator

The Contractor shall act as Node Site Coordinator (NSC), for the designated representative of the sponsoring communications or information systems command or agency. As NSC, The Contractor shall follow DISA Circulars 310-55-9, Chapter 2 for the associated DISA infrastructure as well as DISA Circular 310-70-1. Node Site Coordinator functions are only required at SC HQ, JTF-Bravo, and JTF-GTMO.

5.1.4.4.11 Video Teleconferencing Services (VTC, Briefing and Display Systems, and Conference Room Support)

The Contractor shall operate, maintain, and perform life cycle activities all VTC, briefing and display systems, and conference room systems. The Contractor support for conference room and VTCs shall include a reservation scheduling and coordinating with distant-end participants.

The Contractor shall provide VTC support on a by-location basis in accordance with the phase-in plan developed in paragraph 5.1.1.1. The Contractor shall develop and implement means to remotely manage all VTC systems under this Task Order, which is expected to reduce or eliminate resources supporting Video Teleconferencing Services at appropriate locations. The Contractor shall use existing, develop, or tailor conference room scheduling tools to manage conference rooms and help Users request VTC and other conferencing support.

5.1.4.4.11.1 Public Address Systems Support

The Contractor shall provide public address system support (in addition to operations and maintenance) to include setting up and tearing down systems for all functions and ceremonies as requested via work orders. The estimated number of functions and ceremonies per year at SC HQ is 30. For planning purposes, assume 6 requests for public address systems support per year for JTF-Bravo and 6 requests for JTF-GTMO.

5.1.4.4.11.2 SC HQ IP Television.

The Contractor shall maintain the existing IPTV distribution network at SC HQ. The demarcation point for the cable company is outside the SC HQ. The Contractor shall identify and address any malfunctions with the TV signal inside the SC HQ.

5.1.4.4.12. Satellite Communications Support

The Contractor shall provide the following Satellite Communications Support.

5.1.4.4.12.1 MILSTAR Terminal

The Contractor shall operate, maintain, and assist the Government in life cycle support the MILSTAR Satellite Communications Terminal and associated facility life cycle support activities in accordance with OEM best practices and guidelines. The MILSTAR terminal is only located at the SC HQ facility.

5.1.4.4.12.2 Very Small Aperture Terminal (VSAT) Terminals

The Contractor shall operate, maintain, and life-cycle support Very Small Aperture Terminal (VSAT) networks. The ACOR will approve all procurement actions for the satellite, communication, and terminal services. Connectivity for VSATs and licenses approvals will be provided via DISA and funded by the government. The Contractor shall be responsible for the design, engineering, and all technical coordination with DISA for new capabilities, as well as, all other Government organizations and their vendors. See Attachment 15 for VSAT locations and current fielding status.

5.1.4.4.12.2.1 VSAT Hub Services and Network Management

The VSAT hub is located at the Department of State facility at Brandy Station, VA. The Contractor shall ensure the hub serves as the consolidated theater KU-Band downlink for all designated field sites and the breakout and separation point of the voice and data circuits. When required and following COR approval, the Contractor shall design, coordinate and implement connectivity from the designated US location to SC HQ, theater Networks, and all necessary interfaces with the Department of State Network. The Contractor shall monitor the space segment and circuit usage continually and provide a report to the COR on a monthly basis. The Contractor shall consolidate Monthly Outage Reports with the network monitoring reports. Upon COR request, the Contractor shall provide the utilization reports to the government. The Contractor shall make period assessments that factor network response time and voice usage to accomplish bandwidth increases or decreases to optimize the recurring costs. The Contractor shall provide VSAT network management support on a 40 hours per week basis with a 2 hour response time after duty hour and on weekends. The Contractor shall share outage and trouble ticket information between the SC Service Desk and the VSAT Teleport via telephone and Email.

5.1.4.4.13 Cable Infrastructure Support

The Contractor shall provide vertical and horizontal electrical power, CAT 5, CAT 6, coaxial cable, telephony, and fiber cable infrastructure installation, de-installation, and maintenance support across all rooms and facilities, as well as, patch panels and distribution frames in accordance with commercial best practices, as well as, State and Federal standards. This includes all cable and fiber optic circuits. The Contractor shall also be responsible for power cables in Data Center facilities. Local building codes apply in JTF-Bravo and JTF-GTMO for outside cable plant. The Contractor shall coordinate with the ACORs for outside cable plant installations, modifications, or maintenance at JTF-Bravo and JTF-GTMO.

5.1.4.4.13.1 Cable Infrastructure Support at Department of State Sites

The Contractor shall coordinate with the Department of State, Post Information Management Officer (IMO) and DTS-PO to ensure the necessary cable plant and power is available to meet network needs. In the event that additional support is required, with COR approval, the Contractor shall obtain COR approval for reimbursement and then procure and ship any necessary equipment and provide personnel when necessary to assist in the installation process. The Contractor shall ensure that all acquisitions and construction are accomplished in accordance with DoD and Department of State diplomatic security construction security practices.

5.1.4.4.14 Global Command and Control Systems-Joint (GCCS-J) Systems Operations and Maintenance

The Contractor deployed operational GCCS-J system of record and provides support to the GCCS lab/test facility. The Contractor shall configure and update servers with Government Furnished GCCS-J Family of Programs (FoP) applications and operating systems in accordance with OEM and government provided guidelines. The contractor is responsible for 24X7 on call support of the Command C2 Systems of Record, currently GCCS-J FoP.

5.1.4.4.15 MNIS System Common Operational Picture (COP) Support

The Contractor shall operate and maintain or provide system administrator support functions for the following systems that distribute or process Common Operational Picture information.

5.1.4.4.15.1. Common Operational Picture (COP) System Administrator Support

The Contractor shall operate and maintain deployed systems that provide SECRET and unclassified Common Operational Picture (COP) administration for users of GCCS-J FoP), and the unclassified version for users of CSII. The Contractor shall assist the CSII CONUS administration personnel staff. The Contractor shall provide cleared individuals that are bi-lingual in the Spanish and English languages to assist users with the daily operations and maintenance functions for CSII.

5.1.4.4.15.2 Cooperating Sensor Information Integration (CSII) Maintenance Support

CSII is a commercial product that enables a web based common operational picture. The Contractor shall maintain of the CSII server/s and associated headquarter connectivity equipment. The Contractor shall perform CSII system administration. The Contractor shall conduct troubleshooting on CSII software suite and any hardware on the SC network. The Contractor shall retain reach back support with the CSII OEM and other software developers to maintain and administer CSII and to conduct troubleshooting. The Contractor review and update the accreditation package for CSII. The Contractor shall provide and limit CSII access for specific users. The Contractor shall monitor and log user usage rates and generate a weekly report based on this information. Reports shall include username/nation, IP address accessed from, start/stop time and total time for system administrator during the specified period. (Deliverable #31, Attachment 1)

5.1.4.4.15.3 CSII Integration Support

The Contractor shall support the integration of CSII and the Common Operational Picture (COP) Family of Systems support to the Enterprise. The Contractor shall consult with the CSII PM and CSII developers and provide recommendations on development for cross-domain solutions with an end goal of a unified collaborative environment. The Contractor shall install software upgrades provided by the CSII OEM or other software vendor and coordinate with SRI (or applicable software vendor) to conduct basic and advanced troubleshooting. The Contractor shall provide recommendations on sustainment support and requirements as the CSII program

matures/expands to Full Operational Capability (FOC). The Contractor shall support configuration documentation, development of data sharing policy, and development of procedures to manage data exchanges.

5.1.4.4.15.4 CSII Sensor Integration

When directed by the COR, the Contractor shall integrate additional sensor feeds into the CSII server; it is the responsibility of the Government to ensure that additional sensor feeds meet formatting requirements. The Contractor shall coordinate with external agencies that provide feeds to include US Air Force, Air Combat Command and the Federal Aviation Administration to conduct troubleshooting of local resources on information feeds coming into CSII and shall troubleshoot/maintain the external agency portion of that feed. The Contractor shall develop an advanced/basic CSII software suite troubleshooting flow chart to support O&M and PN training on user interface functions and related approved software applications. (Deliverable #32, Attachment 1)

5.1.4.5 SOUTHCOM Theater Network Coordination Center (TNCC)

The Contractor shall provide personnel to staff the TNCC in order to monitor the theater's communications grid, determine operational impact of degradations and outages within the grid, and to coordinate responses between CYBERCOM, DISA, SC Staff, Components, and Direct Reporting Units with respect to degradations and outages that affect SC operations. The TNCC serves as the primary point of contact for SC regarding communications issues within the SC Theater of Operations.

Contractor personnel operating in the TNCC shall coordinate scheduled system outages and act as the Service Desk after normal hours of operation for the Service Desk. The Contractor shall coordinate restoration responsibilities and priorities with all agencies and respond to inquiries on user incidents involving data on archive systems. The Contractor shall develop a Communications Status (COMSTAT) report on a daily basis identifying all degradations and outages whether planned or unscheduled. (Deliverable # 37, Attachment 1)

5.1.4.6 Life Cycle Replacement or Integration of Hardware or Software

The Contractors Operations and Maintenance Plan shall identify when all Hardware and Software must be replaced as a result of OEM non-supportability. The Contractor shall implement and execute plans to continuously replace Hardware or Software before it no longer supported by the OEM. The Contractor shall assess changing for OEM software for functionally equivalent items as a part of Life Cycle replacement. The Contractor shall seek approval through the normal configuration control board process. (Deliverable # 22 and 58, Attachment 1)

5.1.5 Minimum Performance Requirements

The Contractor shall maintain all systems and services at an accessibility and availability level of 99.85% on a monthly basis; this is the minimum performance requirements for systems and services. This equates to approximately 1 hour per month of down time excluding time for approved service outages or man-made/natural disasters. The availability figure of 99.85% is dependent on network infrastructure such as routers and switches to be operational and as such, the contractor shall measure system availability directly on systems or at a close point. The list of systems and services by location are contained in attachment 9. The availability of infrastructure at the SC locations is also discussed in attachment 9. The Contractor shall identify any systems and services that are not configured to meet this level of availability for COR consideration. If approved, the Contractor may maintain select systems or services at a reduced availability or the COR will provide direction to initiate modifications to increase the availability. The Contractor shall make no changes to increase availability without approval from the appropriate COR. The Contractor shall report performance levels on a by system/service for all locations. The Contractors report shall include changes from the last 6 months for all systems and services. The Contractor shall add new systems to attachment 9 as required after transition to operations. (Deliverable # 34 Attachment 1)

5.1.5.1 Minimum Performance Requirements Formulas and Definitions

The Contractor shall compute all formulas and calculations down to 3 decimal points. A system shall be considered operational even if specific hardware is not functional, if mission users can access required applications and obtain required service and data within an acceptable time frame currently defined as no greater than 3 seconds for data or systems hosted at any location. A system shall be considered non-operational, even if all hardware is operational if mission users cannot access required service and data within the acceptable time frame. Note that these concepts assume that all GFE circuits are operational when considering Cloud Hosted or remote managed services.

Downtime begins when a service or system information is unavailable to any end user. For Server based services, measurement is accomplished at the point closest to the Service given that there may significant interconnection devices for distant users. User devices can be accessed via random sampling. There is no prorating of down time. Down time starts when either: 1) The personnel at the Service Desk are notified of user service or data unavailability or malfunction of systems, or 2) when automated tools report system problems. In all cases the more restrictive measure shall be used.

For all calculations:

1. Down Time = total time (minutes) the system in question is non-operational

2. Availability Percent = [(Maximum System Availability – Down Time)/Maximum System

Availability]*100

3. Maximum System Availability = Total minutes in the performance period – Total minutes of down time

5.1.6. Key Performance Indicators (KPIs)

The Contractor shall develop and implement methods to capture, benchmark, and then monitor the following KPIs for situational awareness, planning, and management decisions. KPIs are not indicators of performance; they are snapshots of system or process capacities. The Contractor shall recommend the frequency and method for presenting the respective KPIs through an automated dashboard. The Contractor may present KPIs in paper format for the first six months of the contract. The Contractor generated KPI report shall include changes from the last 6 months for all systems and services. New systems implemented by the Contractor may require the development or modification of KPIs; the Contractor shall add these to the KPI list after COR/ACOR approval and transition to operations of any new system. (Deliverable # 35, Attachment 1)

5.1.6.1 System Resource Utilization KPIs

The Contractor shall develop, benchmark, then monitor system resource utilization, such as disk configuration, memory, and central processing unit (CPU), on servers, routers, switches, and desktops. The Contractor shall perform desktop analysis at the time of developing baselines or when troubleshooting.

5.1.6.2 Capacity Management KPIs

The Contractor shall develop (forecast), benchmark, and then monitor following capacity Management KPIs for all servers, network storage devices, and network communication devices. For Storage devices, the focus is storage capacity. For Servers (virtual or physical), the focus is processing capacity. For Network devices the focus is bandwidth and latency.

Key Performance Indicator (KPI)	Definition
Incidents due to Capacity Shortages	Number of incidents occurring because of insufficient Server, Storage, or Network Device capacity
Accuracy of Capacity Forecast	Deviation of the predicted capacity from current actual capacity
Capacity Adjustments	Number of adjustments to service and component capacities due to changing demand
Unplanned Capacity Adjustments	Number of unplanned increases to service or component

	capacity as result of capacity bottlenecks
Resolution Time of Capacity Shortage	Resolution time for identified capacity bottlenecks
Capacity Reserves	Percentage of capacity reserves at times of normal and maximum demand
Percentage of Capacity Monitoring	Percentage of services and infrastructure components under capacity monitoring

5.1.6.3 Availability Management KPIs

The Contractor shall develop, benchmark, then monitor the following Availability Management KPIs for all servers (virtual, physical or appliance) based applications, network storage devices, and network communications devices. For servers the focus is availability of voice, data, video, and collaboration applications. For network devices the focus is availability of primary and secondary routing and switching systems.

Key Performance Indicator (KPI)	Definition
Service Availability	Availability of IT Services relative to the availability requirements in the Contract
Number of Service Interruptions	Number of service interruptions
Duration of Service Interruptions	Average duration of service interruptions
Availability Monitoring	Percentage of services and infrastructure components under availability monitoring
Availability Measures	Number of implemented measures with the objective of increasing availability

5.1.6.4 Information Assurance Management KPIs

The Contractor shall develop, benchmark, then monitor the following Information Assurance Management KPIs.

Key Performance Indicator (KPI)	Definition
Number of implemented	Number and description of preventive security measures

Preventive Measures	which were implemented in response to identified security threats. This includes OEM, STIG or IAVM implemented measures.
Implementation Duration	Duration from the identification of a security threat to the implementation of a suitable counter measure
Number of major Security Incidents	Number of identified security incidents, classified by severity category
Number of Security-related Service Downtimes	Number of security incidents causing service interruption or reduced availability
Number of Security Tests	Number of security tests carried out
Number of identified Shortcomings during Security Tests	Number of identified shortcomings in security mechanisms which were identified during tests

5.1.6.5 Bandwidth Metrics

The Contractor shall analyze bandwidth utilization on terrestrial and satellite circuits as well as internal networks and make recommendations for improving network performance. (Deliverable # 36 Attachment 1)

5.1.7 Continuous Process Improvement

The Contractor shall assess and identify improvements for processes, services, systems or network deficiencies. The Contractor shall recommend corrective action, and engineer, integrate, or implement said recommendations as tasked by the COR. Process changes that reduce costs and maintain operational availability as well as system performance to include same levels of Key Performance Indicators are highly encouraged. (Deliverable # 38 Attachment 1)

5.1.7.1 Quality Control Audits

The Contractor shall perform self-audits against the LCIQCP not less frequently than every 6 months from date of award. The Contractor shall identify all areas where the required quality is not met and execute corrective action steps. (Deliverable # 40, Attachment 1)

5.1.7.2 Monthly Analysis of Communications Status (COMSTAT) Network Service Call Report, Service Desk Reports, Logs and KPIs.

The Contractor shall analyze the TNCC-published COMSTAT networks service call report and the Service Desk Logs and reports as well as all key performance indicators. The Contractor shall use the analysis to make recommendations to reduce the number of related future calls by responding to key problems, e.g., refining user training, developing online help screens, and providing input to TNCC. (Deliverable # 37, 39 Attachment 1)

5.1.7.3 Process Improvement Working Group

The Contractor shall support a yearly process improvement working group meeting at SC HQ to present recommendations to increase efficiency or availability of systems to the ACORs. Recommendations that are approved and require modification to the Contract shall be followed by appropriate direction from the COR and or Contracting Officer, otherwise, the Contractor shall take no action. (Deliverable # 38, Attachment 1)

5.1.8. Reserved.

5.1.9 Software Engineering and Integration/ Application Development Life Cycle Support Activities

The Contractor shall execute the following Software Engineering and Integration (SEI)/Applications Development life cycle support activities. The Contractor shall execute SEI activities in accordance with SOUTHCOM SEI standards (see Attachment 24).

The Contractor shall develop and maintain a list of requested SEI application activities to include estimated levels of manpower resource to complete efforts; the Contractor shall provide the prioritization of these activities on a quarterly basis to the ACOR.

(Deliverable 91, Attachment 1)

5.1.9.1 Existing Web Application Life Cycle Support

The Contractor shall assume responsibility of existing Web application life cycle support on an as-is basis. See Attachment 10 for the list of existing applications the Contractor shall maintain under this effort. Given the periodic discontinuance of OEM software development platforms, or the inability of legacy software to operate with updated OEM operating systems or databases, the Contractor shall migrate and modernize applications from existing software baselines to updated versions in order to ensure long term life cycle support. Guidance will be provided on a case-by-case basis to transition any capability to an updated version or through integration of Commercial-off-the-shelf tools. The Contractor shall support the transition of all SOUTHCOM applications to enterprise services upon collapse of the environments, transition to cloud hosted configurations, or integration of IDAM services.

5.1.9.1.1 Existing Application – SC Baseline Compliance

The Contractor shall verify and generate an assessment identifying if existing applications are compliant with the SEI Policy. Guidance will be provided by the COR to transition applications that are not compliant with SEI Policy. (Deliverable #44, Attachment 1)

5.1.9.1.2 JDIMS Application Baseline Documentation and Software Re-Engineering

Due to the significance of the JDIMS application, the Contractor shall accomplish complete assessment and documentation of the JDIMS application in accordance with Paragraph 5.1.9.2 as well as, development to transition the application to an SEI compliant system during the Base Period. This effort shall start after the first Phase-In period. The Government requires 2800 hours during the base period and 3840 hours during Option 1 ~~6740~~ of additional Software Engineering support at USSOUTHCOM HQ (Doral FL) ~~prior to completion of the JTF-GTMO Phase-in Period~~. Contractor support hours on this effort will be exclusive of other SEI or JDIMS activities. The Contractor will be provided a copy of the JDIMS application and may travel to JTF-GTMO if required. See separate CLIN for this effort.

5.1.9.2 New Application Development

The Contractor shall assess, design, develop, integrate, and implement new and existing software applications through a multistep process. This includes planning, initiation, analysis, design, implementation, and sustainment to disposal. For requirements approved by the ACOR, the Contractor shall assess integration of existing Commercial Off-The-Shelf tools before developing custom applications. In addition to documentation normally required during the planning, design, transition, and sustainment phases of a new system (IAW paragraphs 5.1.1, 5.1.2, 5.1.3, and 5.1.4) the Contractor provided documentation shall include a technical requirements package that matches the functional requirements, UML architecture, decision tables to address triggers and situations that are mutually exclusive, as well as an executive summary of the overall design of the application, the database requirements, data validation requirements, internal and external interfaces, authentications, permission architecture, and reports. If applicable, the government shall add new applications to the Minimum Performance Requirements (per paragraph 5.1.5) and Key Performance Indicators Lists (per paragraph 5.1.6) after ACOR approval. (Deliverable 15, Attachment 1)

5.1.9.2.1 SEI Policy Compliance

The contractor shall develop all web applications to be compliant with SEI Policy. The Contractor shall engineer and/or integrate access and security controls to applications in accordance with existing access controls or integrated with the future IdAM capabilities. (Deliverable # 44, Attachment 1)

5.1.9.2.1.1 Custom Application Development Model

The Contractor shall propose the development model to be used for all new application development activities, to be approved by the government. (Deliverable 15, Attachment 1)

5.1.9.2.2 New Application Development using Ozone Widget Framework (OWF) - Option

The Contractor shall provide 1440 Hours during the base period and 1920 Hours/year thereafter of OWF Application Development support for integration of DoD OWF based applications using approved DoD OWF widgets. The Contractor shall assess, design, develop, integrate, and implement new and existing OWF based web sites and dashboards that enable users to access other websites and applications. The Contractor OWF implemented capabilities shall enable users to configure their own web pages with to access information such as e-mail, maps, word processing and spreadsheets or any other database within the SOUTHCOM enterprise, as well as, external DoD databases. The Contractor shall also use OWF widgets to build dashboards for any type of management or operational situational awareness

All OWF application development and integration shall include planning, initiation, analysis, design, implementation, and sustainment to disposal. This effort shall start after the first Phase-In period. Contractor support on this effort will be exclusive of other SEI or JDIMS activities.

5.1.9.3 Application Hosting – Cloud Hosted Services and Hoteling Services

The Contractor shall provide hosted services or hoteling services for applications owned and operated by other organizations. Contractor-provided Hosted services include providing the physical or virtual server environment to include required computing resources, databases and storage for development and live environments, as well as, loading applications onto the live environments. The Contractor shall provide technical assistance to support organizations with implementing PKI authentication and SC access control mechanisms. The list of current Hosted applications is contained in Attachment 10. The Contractor shall verify and maintain this list. (Deliverable #45, Attachment 1)

Hoteling services are also described in Attachment 10. The list of Hoteled applications is not complete; the Contractor shall identify other Hoteled applications during the transition period of each location. The Government may request the Contractor to add new Hosted Applications or Hoteled Application services at any time through normal work order processes.

5.1.10 IT Systems Support Services (ITSSS)

The Contractor shall provide IT Systems Support Services (ITSSS) for key functional areas across the AOR. ITSSS provided by the Contractor are broken into 3 Subcategories. Category 1 is IT Operations and Maintenance (O&M) Support Services. These ITSSS function are not directly part of the operations and maintenance processes but are essential for life cycle support

activities. Category 2 is IT User Support Services. In providing Category 2 ITSSS functions, the Contractor shall accomplish training, adaptation, and IT use advice to Users. Category 3 is Consultants, OEM Certified Partners, and OEM Support Services. In providing OEM Support Service, the Contractor shall accomplish planning or assessments for modifications or anomalies that require Tier 4 support.

The following sub-paragraphs identify specific ITSSS functions to be accomplished by the Contractor. The LCIQCP shall describe how the contractor will manage and document accomplishments and status of all activities performed by ITSSS support personnel. The Contractor shall consolidate and submit activity reports every two weeks for personnel accomplishing ITSSS services. (Deliverable # 41, Attachment 1)

5.1.10.1 IT O&M Support Services

IT O&M Support Services consist of those functions that are not directly tied to maintaining systems but are required to ensure the life-cycle support. The Contractor shall provide the IT O&M Support Services in the following sub-paragraphs. The Contractor shall provide a bi-weekly report of all planned and accomplished activities performed by personnel in these areas. ((Deliverable # 41, Attachment 1)

5.1.10.1.1 Program Management Support

IT Program Management Support is required to ensure financial planning and execution and project management planning and execution functions are synchronized across all efforts. The Contractor shall provide Project Management Support in the following sub-paragraphs:

5.1.10.1.1.1 Contract Management Specialist Support

The Contractor shall develop acquisition packages to include performance work statements, cost estimates, and market research to support the acquisition of systems. (Deliverable # 41, Attachment 1)

5.1.10.1.1.2 Finance and Budget Office Support

USSOUTHCOM obtains funds from the following program sources: 1) Army-sourced COCOM funds, 2) Army-managed Counternarcotics funds, 3) Overseas Contingency funds for JTF-GTMO, 4) Overseas Contingency Operation funds for JTF-Bravo, 5) Program of Records funds for GCCS, Program of Record Funds for Combined Enterprise Regional Information Exchange System (CENTRIXS). From these sources, USSOUTHCOM also manages operations and maintenance funds and procurement funds. For purposes of this effort, these sources are generalized as multi-fund source requirements. The purpose and expenditure of these funds must be tracked and aligned to all contract deliverables or services on this effort.

The Contractor shall develop and maintain ledgers and computer databases to record, track, and develop reports for multiple-fund source requirements executed on this Task Order. Based on trend information developed from databases, government purchase card (GPC) purchases, and contract procurements, the Contractor shall provide input to the resource management staff for yearly budget and program objective memorandum (POM) submission.

(Deliverable # 41, 78, Attachment 1)

5.1.10.1.1.3 Microsoft Enterprise Project Management Technical Support

The Contractor shall provide continuous support to implement and sustain Microsoft Project Management server. When required, the Contractor shall modify existing project templates and associated metadata, as well as, provide training to project managers on using Microsoft Project Management Server. The Contractor shall maintain an integrated schedule of all activities and deliverables for this Task Order, as well as, all projects. (Attachment 1, Deliverable 2)

5.1.10.1.2 Cybersecurity Policy and Defensive Cyber Operations

The Contractor shall execute cybersecurity policies and Defensive Cyber Operations processes to ensure all networks are protected from persistent cyber-attacks, unauthorized access, service interruption and unauthorized disclosure or modification of information that is processed on them. The Contractor shall research, develop and implement a risk management strategy for networks to enable the execution of USSOUTHCOM (USSC) operations. The Contractor shall develop a plan that identifies how they shall execute cybersecurity and data strategies for the USSC Network consistent with DoD and USSC guidance. The Contractor shall execute the following subtasks on existing systems and networks. The Contractor shall assess changes or implementation of the following during planning phase of any transition, modification, expansion or new systems implementation. Within this area, there are two levels of support.

Level 1 Services are associated with Implementing cybersecurity policy(s) and Defensive Cyber Operations. Major efforts are include generating required certifications and accreditation documents in Enterprise Mission Assurance Support Service (eMASS), activity reports, and tracking the implementation of security related configuration changes, as well as, scanning systems at the local levels.

(See Deliverables Matrix # 46, Attachment 1).

Technical Exhibit 19, Attachment 19 contains tables with a list of Accreditation Packages for SIPRNET and NIPNET Networks, VTC Circuits, and Hoteled or Hosted Systems that are being maintained and tracked. The tables identify if a given accreditation package must be developed/maintained and tracked in the case of Level 1 IA Services or just reviewed and

tracked in the case of Level 2 IA Services. These tables are provided to give an idea of the magnitude of the effort; any classified information has been redacted.

5.1.10.1.2.1 Level 1 Support Services.

The Contractor shall accomplish the following services in accordance with DoD Instructions 8500 series, 8510.01 and NIST Special Publications 800-37, 800-53, 800-53A.

5.1.10.1.2.1.1 USCYBERCOM (USCC) Orders, Directives, Vulnerability Alerts, Bulletins and Technical Advisories

The contractor shall track and ensure implementation of USCC Directives to include Operational Orders (OPORDs), Tasking Orders (TASKORDs), Fragmentation Orders (FRAGOs), Warning Orders (WARNORDs) Information Condition (INFOCON); and other "directives" for USSC network assets throughout the theater to include USSOUTHCOM HQ, JTF-Bravo, JTF-GTMO, and 26 individual Security Cooperation Offices (SCOs) in 26 countries and the Washington Field Office. The contractor shall evaluate implementation of all applicable Information Assurance Vulnerability Alerts and Bulletins released IAW US Cyber Command (CYBERCOM) IAVM TASKORDs. The Contractor shall perform analysis, implement, and report the compliancy of Information Conditions (INFOCON) changes and TASKORDs . (See Deliverables Matrix #47, Attachment 1)

5.1.10.1.2.1.2 Security Technical Implementation Guides (STIGS)

The Contractor shall provide periodic STIG analysis and develop plans of action and milestones for implementation after approval. (Deliverable # 48, Attachment 1)

5.1.10.1.2.1.3 Cybersecurity Assessments

The Contractor shall prepare for, assist with, and monitor Cybersecurity assessments, Command Cyber Readiness Inspections, Red and Blue Team assessments, vulnerability scans, certification and accreditation reviews for the command. The Contractor shall develop corrective courses of action for findings identified during assessments for COR or ACOR approval. The Contractor shall resolve open security vulnerabilities in a timely manner focusing on the most critical vulnerabilities first. (Deliverable 49, Attachment 1)

5.1.10.1.2.1.4 Wireless Device Scanning

The Contractor shall accomplish continuous mobile scanning for Unauthorized Wireless intrusion/access points on a monthly and no notice basis.

5.1.10.1.2.1.5 Vulnerability Scans and Checks

The Contractor shall continuously perform vulnerability scans/checks on all SC assets (including Program of Record (POR) systems), and accomplish periodic audits using the installed compliance and vulnerability scanning tools. The Contractor shall evaluate the scan results and mitigate, remediate or waive (exempt from mitigation) security threats. The Contractor shall develop and maintain a log of all accomplished vulnerability scans and actions. (Deliverable # 50, Attachment 1)

5.1.10.1.2.1.6 Web Content Filtering and Monitoring

The Contractor shall support web content filtering, and monitor and control access to prohibited web sites. The contractor shall develop and maintain a log of all accomplished Web Content Filtering and Monitoring. (Deliverable # 51, Attachment 1)

5.1.10.1.2.1.7 Cybersecurity Monitoring Support

The Contractor shall leverage the Cybersecurity Tools to include Firewalls, IPS, IDS, Assured Compliance Assessment Solution (ACAS), HBSS, etc. to accomplish Network Security Monitoring and Intrusion Detection. The Contractor shall detect, monitor and act on malicious activities or policy violations. The Contractor shall document and take appropriate incident response actions. The Contractor shall develop and maintain a log of all accomplished incident actions to include any findings.

The Contractor shall identify cyber indicators and set priorities for significant Cyber events. The Contractor shall make recommendations to fine tune sensors and information assurance devices, as well as, correlate network patterns in order to identify anomalies and the advanced persistent threat.

(Deliverable #52, Attachment 1)

5.1.10.1.2.1.8 Training and Certification of Personnel with Elevated Rights

The Contractor shall ensure all personnel granted elevated privileges or performing IA functions on SC systems/networks are trained and certified in accordance with the DoD Manual 8570.01M, Information Assurance Workforce Improvement Program. The Contractor shall track compliance of all Cybersecurity positions (military, civilians, and Service Providers) to include Program of Record (POR) system administrators, and conduct periodic audits within directory services to resolve discrepancies.

5.1.10.1.2.1.9 Tracking, Reporting and Executing Corrective Acton Procedures for Classified Message Incidents

The Contractor shall report, mitigate, and/or execute corrective action procedures for all classified information incidents (e.g. data spills) that impact SC networks within time constraints

identified in Chairman Joint Chiefs of Staff Manual (CJCSM) 6510.01B, Cyber Incident Handling Program. The contractor shall develop and maintain a log of all Classified Information Incident actions. (Deliverable #53, Attachment 1)

5.1.10.1.2.1.10 Cybersecurity Incident Response Analysis / Attack Sensing and Warning Support.

The Contractor shall accomplish incident response analysis/attack sensing and warning. The Contractor shall analyze static and dynamic anomalous/malicious software. The Contractor shall analyze and correlate anomalous events and host logs in order to assess threats. The Contractor shall collaborate and interface with external organizations/agencies on security related issues and investigations. The Contractor shall respond to known and possible network attacks to mitigate the attack or ensure Services continue or are restored. The Contractor shall report on all network attacks, analysis and responses. (Deliverable # 85, Attachment 1).

5.1.10.1.2.1.10.1 Cybersecurity Forensics Support - Option

The Contractor shall provide forensics support. The Contractor shall reverse engineer anomalous / malicious software to identify root-cause issues that require mitigation. The Contractor shall accomplish preservation, identification, documentation, and interpretation of data on network and hard drives. The Contractor shall collect, preserve, and transfer forensic evidence of unauthorized access to support Law Enforcements and Counter Intelligence investigations. (Deliverable # 96, Attachment 1).

5.1.10.1.2.1.11 Network Security Event Log

The Contractor shall archive and audit network security event logs. The Contractor shall provide firewall logs, system logs, and associated media to designated organizations in the performance of forensic analysis services. (Deliverable # 54, Attachment 1)

5.1.10.1.2.1.12. Communications Security (COMSEC) Support

The Contractor shall provide technical advice and assistance for implementing the COMSEC programs. This includes providing communications security account management for special customer accounts held throughout the SOUTHCOM AOR. The Contractor shall ship and receive Controlled Cryptographic Item (CCI) devices through the Department of State COMSEC account and the Defense Courier Service (DCS). The Contractor shall track and maintain accountability of all COMSEC material (Electronic KEYMAT) and Controlled CCIdevices in the SOUTHCOM AOR. (Deliverable # 30, Attachment 1)

5.1.10.1.2.1.13 COMSEC Logistics

The Contractor shall, receive, ship, and hand receipt US and releasable COMSEC keying material, as well as, associated key transfer devices, through DoD and State Department authorized shipping channels.

5.1.10.1.2.1.14 Accreditation Packages

The Contractor shall accomplish certification and accreditation of DoD IS, platform IT (PIT), IT services, and IT products, in accordance with DoD 8510.01. The Contractor shall accomplish, maintain and update all Level 1 Information Assurance accreditation packages and system security authorization agreements. The Contractor shall develop a schedule for the maintenance and update of all packages in accordance with the DoD Risk Management Framework. See Attachment 19 for current list of level 1 Information assurance packages. (Deliverable #100, Attachment 1)

5.1.10.1.3 Configuration Management

The Contractor shall maintain a configuration management (CM) system to include a configuration management plan that outlines processes for detailed recording and updating of information related to hardware and software for all networks. (Deliverable #57, Attachment 1)

5.1.10.1.3.1 Configuration Control and Change Board

The Contractor shall establish and maintain Configuration Controls and support a Government managed Configuration Change Control Board (CCCB). The CCCB is the Government's means to evaluate all change requests and change proposals, and then provide subsequent approval or disapproval. The Contractor shall process all modifications to the system's design, hardware, firmware, software, and documentation through the CCCB. The Contractor shall formally submit and track requests to alter the configuration. (Deliverable #58, Attachment 1)

5.1.10.1.3.2 System Documentation - Approved Baseline Documentation

The Contractor shall document and maintain COR-approved software and hardware baselines. The Contractor shall maintain “as-built” and “as-configured” system configurations, on all the devices to include networks switches, routers, servers, personal computer baselines, storage devices/system. The Contractor shall only change device configurations after documentation is approved. The Contractor shall also maintain: system evaluation reports, certifications to operate, accreditation packages, and system security authorization agreements. (Deliverable #59, Attachment 1)

5.1.10.1.3.3 Systems Installation Drawings

The Contractor shall take over maintenance of existing drawings. The Contractor shall develop and maintain all engineering drawings in Microsoft VISIO. Some locations may be using other systems such as AutoCAD. The Contractor shall convert all drawings to VISIO within 2 years. (Deliverable # 59, Attachment 1)

5.1.10.1.3.4 Physical Configuration Audit

The Contractor shall perform Physical Configuration Audits (PCAs) at each site in the AOR. The Contractor shall perform PCAs of SCHQ, JTF-Bravo and JTF-GTMO once per year. The Contractor shall audit each SCO every 3 years. The Contractor shall verify and maintain the drawing package for each site. (Deliverable # 60 Attachment 1)

5.1.10.1.4 Property Book Office/Warehouse and Acquisition Support.

The Contractor shall develop and execute a plan to maintain property books, support the operation of warehouses and provide research in acquiring new systems or life-cycle replacements. The Contractor shall execute the following sub-tasks:

5.1.10.1.4.1 Procurement Support

The Contractor shall provide procurement support by assisting the COR in procurement requirements to include contract development and contract renewals. The Contractor shall conduct research on purchases made by government purchase card holders and track procurement of supplies, services, and information technology equipment. The Contractor shall update the organization's purchase log data base and provide reports on the status of orders to include order dates, vendor estimate delivery dates and delivery of supplies and equipment to the end user. The Contractor shall work in coordination with the ACOR to assist in preparation of contract requirements to include developing service contract approvals, justifications, independent cost estimates, market research and other contract specific documents as required. The Contractor shall coordinate with SC personnel and external agencies for establishment of requirements and determining availability of appropriate funding. The Contractor shall maintain records and logs in existing Contract Management computer database(s) on all procurements and contracts executed on this effort from initial submission through completion of tasks.

5.1.10.1.4.2 Accomplish Purchase Order Execution

The Contractor shall issue purchase orders and provide receiving reports to the Resource Management Office at each location. The Contractor shall make recommendations to the ACOR on which items shall be considered IT/IM property book accountable items and upon approval, process items in Global Combat Support System – Army (GCSS-Army).

5.1.10.1.4.3 Contractor Life Cycle Procurement of Hardware, Software, Warrantees and Spare Parts

The Contractor shall develop a life cycle procurement plan that includes timing, volume, and cost estimates for life-cycle replacement and routine spare-parts provisioning of all hardware, software, and warrantees supported on this Task Order. The Contractor shall address timing and cost estimates for licenses and warranties within the plan.

The Government may choose to accomplish procurement of any portion of Hardware, Software, Spare Parts and warrantees and provide them as GFE if it is determined to be advantageous to the Government.

If approved by COR, the Contractor shall procure technical refresh hardware and software, as well as, repair parts and expendables to ensure the life cycle of all components; the Contractor shall demonstrate that the costs for any item purchased is equal to or less than the costs the Government would pay if procured directly.

The Contractor shall obtain required documentation for tax exemption status for all material purchases for the Government's account.

The Contractor shall utilize ESI source software and CHESS contract source equipment. In situations where the purchase of new commercial of the shelf (COTS) hardware and related software (not provisioned under the DoD ESI agreement) is needed to satisfy the requirements of this Task Order, the CHESS hardware contracts are the preferred source of supply. In the event the hardware and related software is not available from a CHESS contract, the Contractor is authorized to obtain the hardware through an alternate source. A waiver is required for the purchase of products from another source valued at over $25,000. The waiver process is located at https://chess.army.mil/ascp/commerce/ESI/waiver/waiverExplanation.jsp.

For IT procurements, the Contractor shall follow HQDA-CIO/G-6 policy. The Program Director (PD) CHESS is the designated primary source for commercial IT products. Procurements of IT hardware or software not utilizing PD CHESS shall require the Contractor to submit a Goal 1 Waiver (G1W) through HQDA-CIO/G-6 via the following website:

https://adminapps.hqda.pentagon.mil/akmg1w/index.html. A copy of the waiver shall be included with the request to the COR/KO.

In the event the hardware and related software is not available from an Army or DOD contract, the Contractor shall obtain COR approval to obtain the hardware or software through an alternate source. In this case the contractor shall acquire the hardware or software through the General Services Administration (GSA) Federal Supply Schedule (FSS) program. Only if the hardware or software is not available via Army or DOD contract, the contractor will acquire the hardware or software via the open market. In the event the contractor is to acquire the

hardware or software via GSA FSS contracts or on the open market, the Contractor shall provide the COR/KO with three valid quotes from three different vendors. For all non-DoD CHESS purchases, the Contractor shall follow the requirements of in the FAR and DFAR obtaining 3 quotes for procurement actions.* The Contractor must provide sole source justification if the availability of the product or service is through a single vendor.

Prior to procurement of any hardware, software, or other item, the Contractor shall notify the COR of the part number, description, proposed source of supply, quantity to be purchased, and value based on the quantity of each part and total quantity price.

The Contractor shall obtain a waiver for the purchase of products valued at over $25,000 from a means other than CHESS. The waiver process is currently located at TO BE FILLED IN DURING PHASE-IN PERIOD. The COR will provide an updated location for the waiver process, if necessary.

For non-ELA or non-CHESS purchases over $25,000, the Contractor shall submit the purchase request, approved waiver and a copy of at least three quotes, to the COR, and procure only after approval is granted by the COR.

The Department of Defense Activity Address Code (DODAAC) is W90P20.

*FAR 13.003 (b)(1)(1) Each Acquisition of supplies or services that has an anticipated dollar value exceeding $3,000. ($15,000 for acquisitions as described in 13.201(g)(1) and not exceeding $150,000 ($300,000 for acquisitions described in paragraph (1) of the Simplified Acquisition Threshold definition 2.101) is reserved exclusively for small business concerns and shall be set aside (see 19.000, 19.203, and subpart 19.5). See 19.000(b) and 19.502-2 for exceptions.

FAR 13.104(b) If using simplified acquisition procedures and not providing access to the notice of proposed contract action and solicitation information through the Government wide point of entry (GPE), maximum practicable competition ordinarily can be obtained by soliciting quotations or offers from sources within the local trade area. Unless the contract action requires synopsis pursuant to 5.101 and an exception under 5.202 is not applicable, consider solicitation of at least three sources to promote competition to the maximum extent practicable. Whenever practicable, request quotations or offers from two sources not included in the previous solicitation.

(Deliverable # 62, Attachment 1)

5.1.10.1.4.4 Inventory of Spare Parts, Consumable, Material and Re-order Point Levels

The Contractor shall develop and maintain a supply inventory of spare parts, expendables parts, and consumables; these items shall be maintained in a current list and approved by the COR.

The Contractor shall ensure that materials are available to complete routine service orders and emergency restorations.

The Contractor shall identify and maintain reorder point levels for all SC sites. The Contractor shall send equipment back to OEMs for warranty repair to the maximum extent possible before ordering replacements.

(Deliverable # 63, Attachment 1)

5.1.10.1.4.5 Licenses and Warranties.

The Contractor shall maintain accountability and tracking of all IT equipment, warranties and software licenses. The Contractor shall obtain software and other required licenses for life-cycle upgrades from approved Government sources. The Contractor shall procure COTS software and equipment during contingencies based on COR direction.

The Contractor shall also procure warranties for IT systems. Within 90 Days of assumption of responsibilities of each site, the Contractor shall survey all IT components for licenses and warrantees to be purchased on a reimbursable basis and provide quotes to the COR for approval.

(Deliverable #64, Attachment 1)

5.1.10.1.4.6 Excess Materials

The Contractor shall inventory any excess materials. The Contractor shall disposition excess material in accordance with COR instructions.

5.1.10.1.4.7 Service Desk Database Update

The Contractor shall update the Service Desk database as appropriate with new equipment or materials as approved by the COR.

5.1.10.1.4.8 Government Property Book Officer (PBO) Liaison

The Contractor shall serve as liaison and subject-matter expert to the SCJ6, 525TH Signal Company, JTF-Bravo, and JTF-GTMO Government Supply and Services supervisors and Government Property Book Officer (PBO) on issues pertaining to logistics management, lifecycle management, warranty item management, and configuration management. GCSS-Army is being fielded to replace the Property Book Unit Supply Enhanced (PBUSE) system. The Contractor shall maintain the GCSS-Army System database current with all SC IT assets.

5.1.10.1.5 Logistics Support

The Contractor shall develop a plan and execute logistics support (LS) for all IT systems. The Contractor shall perform LS functions at contractor or government facilities in Doral, Florida. (Deliverable #79, Attachment 1)

5.1.10.1.5.1 Department of State Certified Warehouse - Option.

The Contractor shall provide and maintain a Department of State (DoS) certified warehouse, with no less than 15,000 square feet. The Contractor shall locate the warehouse within 3 miles of SC headquarters. The Government may provide GFE warehouse space that meets this requirement.

5.1.10.1.5.2 Packaging, Packing and Shipping

The Contractor shall package and preserve all stored or transported IT equipment, using Best Commercial Practice guidelines. When shipping to a SCO, the Contractor shall follow Department of State (DoS) rules for government COMSEC and IT being introduced into Controlled Access Areas (CAA). The Contractor shall coordinate with the DoS and the SC Property Book Offices for packaging, preserving, and shipping the digital and associated construction materials required for installation of IT systems. The Contractor shall transport the SC IT equipment from the staging point to the carrier. The Contractor shall obtain Defense Courier authorization cards for personnel within the SC AOR to escort appropriate shipments.

5.1.10.1.5.3 Transportation

The Contractor shall develop and execute a Transportation Plan to ship all IT equipment as required throughout the AOR or back to OEMs for warranty repair. (Deliverable 71, Attachment 1)

5.1.10.1.5.3.1 Coordination of Shipping for Overseas Shipments

The Contractor shall coordinate the issuance, repair and return, and positioning (inventory control) of SC IT hardware within the SC AOR. For equipment bound for SCOs, The Contractor shall utilize DoS Diplomatic Pouching procedures and schedules for transporting repairable equipment to and from diplomatic locations within SC AOR. The Contractor shall ensure that all COMSEC items destined for installation within an Embassy/Consulate are processed through the DoS COMSEC Vault prior to shipment via classified pouch or diplomatic courier. The Contractor shall appropriately mark Cryptographic Control Items (CCI) for shipping through the diplomatic pouch. The Contractor shall adhere to all DoS procedures for shipments to or from diplomatic locations. The Contractor shall coordinate the transportation of SC IT hardware and/or software with the ACOR.

5.1.10.1.5.3.2 Shipping to US Embassies

The Diplomatic Pouching schedule can and will be changed without prior notice from the DoS. The Contractor shall coordinate with the DoS Diplomatic Security Courier Liaison office to ensure currency of pouch schedule information. The Contractor shall ship via military or commercial means all other SOUTHCOM C4S hardware and software to locations not requiring diplomatic pouching. The Contractor shall stage the SOUTHCOM C4S equipment for installation and coordinate its shipment with the COR and the receiving OSTR and PBO to ensure equipment is exonerated from Host Nation customs and plans are in place to transport equipment to/from airport to/from OCONUS staging location.

5.1.10.1.5.3.3 Escort of Equipment in Department of State Controlled Access Areas

The Contractor shall provide an escort for all equipment shipments destined for installation in a Controlled Access Area (CAA) in accordance with DoS rules and regulations. The Contractor shall coordinate SOUTHCOM C4I reparable equipment at all repair sources (i.e., organic, OEM, other established Government depots) as well as the coordination of OEM warranty actions. The Government will provide a Transportation Account Code (TAC) for Military Air shipments. The Contractor shall provide a price estimate for packaging and transport of other SOUTHCOM related equipment by pouch, commercial or military air (MILAIR). Upon COR approval The Contractor shall package and ship the equipment to SOUTHCOM AOR location(s).

5.1.10.1.5.4 VSAT Logistics

The Contractor shall pack, crate and ship all equipment; shipping is accomplished on a cost reimbursable basis. Damage or loss of equipment shall be the responsibility of the Contractor and shall not affect project costs or schedules; the Contractor shall obtain insurance to cover this contingency; insurance for this purpose is an allowable ODC.

5.1.10.2 IT User Support Services.

The Contractor shall provide the following training, adaptation, and IT use advice to Users.

5.1.10.2.1 Sustainment Training

The Contractor shall train end users in the operation and use of systems and equipment. The Contractor shall provide training on a scheduled basis at all locations. The Contractor shall assume responsibility to maintain and update the existing instructional packages for the following courses: MS Word, MS Excel, MS Outlook, MS PowerPoint, MS Access, MS SharePoint, MS Project, Adobe Photoshop Elements, Conference Room Operations, LAN User Course, DMS/AMHS, Defense Connect On-line, and the Tasker Systems. The Contractor shall furnish instructional handouts and course completion certificates to the students. The contractor

shall standardize the existing Local Area Network Users course for use across the AOR with tailoring on a by-site basis. (Deliverable #43, Attachment 1)

5.1.10.2.1.1 Training Facilities

The Contractor shall operate a training room located at the SC HQ. Training in JTF-GTMO and JTF-Bravo shall be provided in available conference rooms. The Government may create dedicated training rooms in the future at JTF-Bravo and JTF-GTMO. The contractor shall accomplish training for all other locations via Defense Connect Online or equivalent Enterprise Service. On occasion, training may be required in large conference rooms.

5.1.10.2.1.2 Ad-Hoc Training Material

The Contractor shall create ad-hoc instruction for specific groups of members as directed by the ACOR. The Contractor shall provide an assessment of impacts to existing on-going training if ad-hoc training is requested.

5.1.10.2.1.3 Training Material Maintenance

The Contractor shall review documentation, course material, and software changes and update training materials to reflect changes. The Contractor shall coordinate with the Service Desk, system administrators, and technicians with respect to problems faced by customers on a regular basis and include discussion of these issues within the curriculum. The Contractor shall keep abreast of the latest LAN policies and procedures and add them to the curriculum when required. The Contractor shall review Microsoft's training Web site to identify new features that could be incorporated into the curriculum; and review student evaluations and suggest ways to improve courses.

5.1.10.2.1.4 Specialized Multinational Training

The Contractor shall provide PNN, CSII, and Collaborative Portal (SharePoint and other collaborative tools) training. The contractor shall update and maintain User manuals and technical documentation for PNN/SharePoint/CSII in English, Spanish, French, and Portuguese.

5.1.10.2.2. Multi-National Information Sharing (MNIS) User Support.

The Contractor shall provide Multi-National Information Sharing (MNIS) support for SOUTHCOM headquarters, Navy SOUTH (NAVSO) at Naval Air Station, Mayport, FL and SCO-Colombia MNIS CENTRIXS sites in Attachment 16. Contractor tasks shall include maintaining close liaison with the SCJ6 Staff, NAVSO Staff, and the SCO Commander supporting meetings and conferences related to multinational-operations; coordinating and preparing plans and annexes for on-going or near term contingency operations. The Contractor shall perform maintenance and logistics tasks in NAVSO and SCO Colombia. The Contractor MNIS Support

shall include developing and presenting multinational operations-related recommendations to senior leadership based on operational assessments; resolve procedural and operational problems; as well as, respond to and track recurring and nonrecurring User, Maintenance or Logistics issues related to use of MNIS systems at NAVSO, as well as the SCO Commanders and SCJ6 staff elements.

Historical support has entailed two resources in Colombia and one in Mayport to support O&M and logistical activities throughout the USSOUTHCOM AOR. In regards to Inter-American Naval Telecommunications Network (IANTN), this support includes supporting host nation users and assets in over 15 countries throughout the USSOUTHCOM AOR. Due to the ongoing migration from Bi-lateral Colombia (BLCOL) CENTRIXS to Battlefield Information Collection and Exploitation Systems –Extended (BICES-X), the majority of support currently provided by the MNIS OSTR in Colombia is dedicated to the decommissioning of all BLCOL CENTRIXS assets within the country of Colombia. The decommissioning of BLCOL CENTRIXS commenced in 2015 and was expected to be completed by the end of CY16, but the decommissioning has been delayed. A list of CENTRIXS assets in Colombia can be found below:

ROUTERS…….....23
SWITCHES…….……...52
CRYPTO……....42
VOICE OVER IP PHONES…….70
WORKSTATIONS…….....96
PRINTERS…….....67
SCANNERS……...56
VSATS……....06
SERVERS……..09
SECURE VIDEOTELECONFERENCE.….17

5.1.10.2.3 Global Command and Control Systems-Joint (GCCS-J) J6 User Support

The Contractor shall provide User-related support for the Global Command and Control Systems-Joint (GCCS-J) Common Operational Picture (COP) Family of Systems on the SIPR and NIPR networks. The Contractor shall perform daily checks of the system and ensure the Joint Operations Center is supported with accurate and timely data including track data and overlays on SC GCCS systems. The Contractor shall ensure data transmission, reception, and correlation processes for GCCS-J data are executed. The Contractor shall provide on-site training support to Users of the GCCS-J system. The Contractor shall serve as User interface

between Components, JTFs and SC HQ for coordinating, troubleshooting and enhancing data exchanged through GCCS-J. The Contractor shall produce information papers, assessment of plans, concepts of operations, and operational taskings, operator smart books, operator standing operating procedures, and checklists. The Contractor shall maintain and administer the GCCS-J Common Operational Picture (COP) communications configuration, supporting documentation, policy, and procedural management such as filter, interpret, manipulate, name and track COP data/messages. The Contractor shall establish and provide quality control for COP air, land and sea tracks and coordinate with appropriate Component/JTF LNO's to ensure SOUTHCOM track reporting requirements are met. The Contractor shall provide assistance to Common Tactical Picture (CTP) development and track managers internal and external to the command.

5.1.10.2.4 Reserved

5.1.10.2.5. CSII User Support

The Contractor shall provide instructions for users who want to use CSII approved optional applications such as desktop chat client or Google Earth plug-in on how to set up their systems for these applications to work with CSII.

5.1.10.2.5.1 CSII User Access Control

CSII uses commercial off-the-shelf token devices. The Contractor shall issue and manage tokens to authenticate users as members of specific communities of interest upon direction of ACOR. The Contractor shall be responsible for the activation/deactivation of tokens, and addressing user issues associated with tokens.

5.1.10.2.6 SharePoint and APAN Web Portal Support

The Contractor shall provide technical advice, and assistance for implementing the SharePoint and APAN Collaborative portals in the SC AOR. The Contractor shall support users in creating new sites, administering permissions, supporting registration for access, helping with site tailoring, providing one-on-one training, as well as, supporting exercises and conferences requiring collaborative portal support. The Contractor shall periodically search SharePoint sites and report any files which are improperly stored in libraries that are not appropriately labeled or locked down for the classification and need to know level of the information, specifically Privacy Act or Classified Data. The Contractor shall develop and maintain a log of all SharePoint and APAN activities accomplished. (Deliverable # 56, Attachment 1)

5.1.10.3 Consulting and OEM Support Services

The Contractor shall address the need for OEM or other Consulting Services during efforts with significant system change (examples: Life Cycle Upgrades, JIE Transformation, or ~~Network~~

Domain Deprecation), as well as, periodic engagements from Consultants or OEM (or OEM Certified Partners) for Service Operations. At the direction of the Government, the Contractor shall provide or accept as Government Furnished Services, OEM Support Services as required for IT Life Cycle, Software Engineering and Integration, New Capability, or corrective action in order to support planning, engineering, integration, modifications, or assessments that necessitate Tier 4 support. In addition to project/work status reports, the Contractor shall report and forecast monthly hours or funds expenditures for all Consultants or OEM Support Services. OEM support may be provided by OEMs or OEM Certified Gold Partners. OEM Certified Gold Partner to the maximum extent possible; the Contractor will demonstrate that the technical support is of a nature that only OEM can provide the services and the OEM Certified Partners or that the cost is the same. (Deliverable #70, Attachment 1)

5.1.10.3.1 Specialized or OEM Product Consulting Services

The Contractor may utilize consulting services support through OEM or OEM Certified Gold Partners in implementation of planning, engineering, design, integration, or transition of any installed system. The contractor shall justify the need for OEM product support in appropriate planning documents. (Deliverables 3, 10, 11, 13, 15, Attachment 1)

5.1.10.3.2 Consultants or OEM Service Operations Technical Support

If required and approved, the Contractor shall augment Service Operations with support from Consultants, OEM, or OEM Certified Gold Partners in implementation of Service Operations (Known as Premier Services) best practices, as well as, accomplishment of STIG and CYBERCOM orders, directives and (IAVM) notices on specific OEM systems or products. OEM Service Operations Support shall be used to provide independent assessments to ensure that systems are properly configured. Contractor-managed OEM Service Providers shall deliver reports and briefings describing their accomplishments after each engagement. The Contractor shall address the need for periodic engagements from OEM Service Operations technical support contractors as part of the Operations and Maintenance Plan. The Contractor shall utilize Premier Services as required to include pre-planned routine, expedited, or round-the-clock support coverage for high-severity incidents. The contractor shall recommend and periodically update the level of effort for Service Operations Technical Support in the Service Operations Plan. Note that the Government may choose to provide any of the following these services through a different contract vehicle if it is more advantageous to the Government. (Deliverables 10, Attachment 1)

5.1.11 Other Required Support Colombia, JTF-Bravo, JTF-GTMO

5.1.11.1 JTF-Bravo Unique Support

See Part 7 – Attachment 22.

5.1.11.2 JTF-GTMO Unique Support

See Part 7 – Attachment 23.

5.1.11.3 Colombia MNIS and CENTRIXS Operations and Maintenance Support

The Contractor shall provide operation and maintenance support to designated MNIS and CENTRIXS IT equipment in Colombia. The list and location of MNIS equipment in Colombia is contained in Attachment 16.

5.2 On-Site, Off-Site, On-Call, Normal and Emergency Support

The contractor shall provide permanent on-site, off-site, and on-call support in accordance with the by-location minimum requirements as detailed at Attachment 8.

5.2.1 On-Site Support

The Contractor shall provide on-site system and network administration, as well as, Tier 1 and Tier 2, during normal local duty hours (0600 to 1800, Monday through Friday). These hours may be covered on a shift schedule. Contractor network problem identification and response times during normal duty hours shall be within 15 minutes. Once integrated across all locations, the integrated Service Desk shall operate from 0500 to 2000 EST.

The Contractor shall provide services at the TNCC and Technical Control Facility at SC HQ 24 hours per day, 7 days a week.

The Contractor shall provide conference room and VTC support from 0600-1900 local time. For CONUS sites and Joint Task Forces, the Contractor shall provide a two-hour response time after hours and on holidays.

5.2.2 Off-Site Support

The Contractor shall provide off-site system and network administration, as well as, Tier 1 and Tier 2 service on a scheduled or as-needed basis. For locations with Off-Site support, the Contractor shall provide twenty-four hour response time to service degradation or outages that cannot be managed remotely, country clearance process permitting.

5.2.3 On-Call Support

The Contractor shall provide on-call duty to address system outages, security incidents, or classified message incident for any location in the AOR. Response times for any service outage

will be 1 hour and the associated on-call technical support shall be on-site within 2 hours if required for On-Site support sites or as appropriate for Off-Site support sites depending on travel requirements. Upon receiving notification, the Contractor shall initiate actions to resolve major outages within two working hours of receipt of such notice, with the intent of restoring services as soon as possible. Any outage which affects VIPs or Operations Center (in accordance with paragraph 5.1.4.2.5) is also defined as a major outage. The Contractor shall provide a daily and a consolidated quarterly on-call response/incident report.

(See Deliverable # 83, Attachment 1)

5.2.4 Performance of Services during National Crisis Declared by the President or Secretary of Defense

The performance of all services is considered to be “mission essential” during times of crisis.

5.2.5 Performance of Services during Contingency, and Exercise Situations.

The Contractor shall provide system administrator, helpdesk, VTC, and other services during real-world contingencies as well as during exercises. The Contractor shall ensure key personnel remain on-site at respective locations during a hurricane or destructive weather situation to maintain or oversee networks along with identified government personnel. The contractor shall ensure all contractor personnel comply with and abide by the Government’s alert roster reporting procedures. The Government reserves the right to supplement performance of contract functions with Government personnel during periods of disaster, war emergencies, police actions, or acts of nature.

5.2.5.1 Remote Site Recovery

The SC data center has a Data Replication in Support of Continuity of Operations (DRSC) capability. This capability allows the servers and storage systems at SC HQ to replicate information to like equipment at a DISA data center. The Contractor shall accomplish remote site NIPR/SIPR recovery of systems capable of this feature during automatic failover of systems or during emergency situations. The Contractor shall develop and maintain plans describing actions for remote site recovery. The Contractor shall review each plan annually and update as changes occur. The Contractor shall deliver a report addressing the results after each remote site recovery action.

(Deliverable 67, Attachment 1)

5.2.5.2 Failover Testing

The Contractor shall accomplish failover testing to internal backup systems and to external replication sites. The Contractor shall accomplish tests quarterly. The Contractor shall

document and submit the test results and required corrective action for approval. The Contractor shall correct all deficiencies within 30 days. The Contractor shall take actions to not repeat corrected deficiencies.

(Deliverable # 68 Attachment 1)

5.2.5.3 Contingency and Emergency Planning.

The Contractor shall develop and maintain a Contingency Plan that ensures continued performance 24/7/365 in the event of catastrophic and non-catastrophic events and work stoppages. The Contractor shall make the Contingency Plan available for review within four (4) duty hours of request. The Contingency Plan shall address immediate response to catastrophic events to ensure minimal impact on the mission. Contingency situations may require no-notice recall of Contractor personnel to augment shifts and enhance operational continuity in times of national emergency or international crisis as determined by the COR. The Contractor shall provide continuity of mission support in contract performance, or to participate in technical discussions at other locations which may include backup locations as approved by the COR. The Contractor shall coordinate all proposed changes through the COR prior to implementation.

(Deliverable # 66 Attachment 1)

5.2.5.4 Inclement Weather or other Natural or Manmade Disasters Emergency Services

The Contractor shall update and maintain the current plans and operating instructions to address inclement weather phenomena emergency actions, equipment malfunctions, fire, and natural disasters. The Contractor shall address this subject in the Operations and Maintenance Plan.

5.2.5.5 Contingency and Exercise Supplemental IT Support Services

When directed by the COR, the Contractor shall provide additional IT support services as required to support contingencies and exercises.

5.3 Special Requirements

5.3.1 Commercial Internet Service Provider (ISP)

SC provides multinational information sharing systems to foreign countries in support of theater security cooperation activities. The Contractor shall provide connectivity to the Internet to ensure systems are inter-operable. The Contractor shall provide connectivity for the US-owned IT systems fielded in designated OCONUS countries throughout the SC AOR and designated CONUS locations. The Contractor shall assist the Government to obtain quotes from the local, Host Nation or US Internet Service Providers. The connectivity for all sites shall be determined

by the government, but shall be no less than 128kbs for all circuits. The Contractor shall send all requests for ISP connectivity to the ACOR for approval. In addition to the sites listed in Attachment 17, new locations may be identified by the ACOR.

(Deliverable # 69 Attachment 1)

5.3.2 TEMPEST Requirements

The following requirements are on a case-by-case basis for equipment to be placed at US Embassy locations. The Contractor shall work with the ACOR to obtain specific guidance on a by-location basis.

5.3.2.1 Provision or Use of IT

The Contractor shall provide or use only information technology devices or products, as specified by the Government, that have been accredited to meet the appropriate information assurance requirements of The National Security Agency National TEMPEST Standards (NACSEM No. 5100 or NACSEM No. 5100A, Compromising Emanations Laboratory Test Standard, Electromagnetic).

5.3.2.2 TEMPEST Accreditation

Upon request of the COR, The Contractor shall provide documentation supporting tempest accreditation. The Government may, as part of its inspection and acceptance, conduct additional tests to ensure that information technology delivered under this Task Order satisfies the information assurance standards specified. The Government may conduct additional tests if required using certified DoD agencies.

5.3.3 Invoice

The Contractor shall submit an Invoice on a monthly basis.

5.4 Catastrophic Recovery and Support Acquisition Requirements

In addition to supporting IT life cycle activities or new IT capability purchasing requirements, the Contractor shall obtain replacement hardware and software required to perform this order as needed during catastrophic recovery and support. A catastrophe for the purposes of this order is if a critical IT network component fails and cannot be timely replaced by other contracting means. The Contractor shall submit all materiel acquisition requests in advance and in writing to the COR for approval. Equipment purchased by The Contractor under this Task Order shall require Information Assurance Vulnerability Assessment (IAVA) scanning and patching prior to allowing connectivity to the Government production network. Items obtained shall become the property of the Government; the Contractor shall add these items to the appropriate property

book records. The Contractor shall establish a Government-furnished property (GFP) hand-receipt using the GCSS-Army System with the supporting Property Book Officer (PBO). The Contractor shall only acquire material that is in support of the service of this Task Order.

The Government pre-establishes the ceiling for this support at ___TO BE FILLED IN AT CONTRACT AWARD_____ per period.

5.5 Contractor Response at Off-Site Locations

Due to the requirement to perform at travel locations throughout the SC AOR and various CONUS locations, responsiveness shall be defined as that Contractor action which can be reasonably provided as quickly as possible taking into account all specific unique transportation requirements. In all cases requiring travel the Contractor shall respond to the government with both a plan and site action within 24 hours exclusive of travel time or within 48 hours when notification is on a weekend or government holiday. For purposes of this effort, normal duty hours are eight hours per day, local time at site of performance, Monday through Friday excluding government holidays.

5.6 Meetings and Conferences

The Contractor shall attend working group meetings, technical meetings, conference reviews, and seminars as required to support this PWS. The Contractor shall submit a trip report within five working days report following attendance at meetings, conferences, or seminars. (Deliverable #84, Attachment 1)

5.7 Contractor Manpower Reporting (CMR)

The Office of the Assistant Secretary of the Army (Manpower & Reserve Affairs) operates and maintains a secure Army data collection site where The Contractor shall report ALL Contractor manpower (including subcontractor manpower) required for performance of this Task Order. The Contractor shall completely fill in all the information in the format using the following web address https://Contractormanpower.army.pentagon.mil. The required information includes: (1) Contracting Office, Contracting Officer, Contracting Officer's Technical Representative (ACOR) or also known as the Contracting Officer's Representative (COR); (2) Contract number, including task and delivery order number; (3) Beginning and ending dates covered by reporting period; (4) Contractor's name, address, phone number, e-mail address, identity of Contractor employee entering data; (5) Estimated direct labor hours (including sub-Contractors); (6) Estimated direct labor dollars paid this reporting period (including sub-Contractors); (7) Total payments (including sub-Contractors); (8) Predominant Federal Service Code (FSC) reflecting services provided by Contractor (and separate predominant FSC for each sub-Contractor if different); (9) Estimated data collection cost; (10) Organizational title associated with the Unit Identification Code (UIC) for the Army Requiring Activity (the Army Requiring Activity is responsible for providing The Contractor with its UIC for the purposes of reporting this

information); (11) Locations where Contractor and sub-Contractors perform the work (specified by zip code in the United States and nearest city, country, when in an overseas location, using standardized nomenclature provided on website); (12) Presence of deployment or contingency contract language; and (13) Number of Contractor and sub- Contractor personnel deployed in theater this reporting period (by country). As part of its submission, The Contractor shall provide the estimated total cost (if any) incurred to comply with this reporting requirement. Reporting period shall be the period of performance not to exceed 12 months ending September 30 of each government fiscal year and shall be reported by 31 October of each calendar year. Contractors may use a direct XML data transfer to the database server or fill in the fields on the website. The XML direct transfer is a format for transferring files from a Contractor's system to the secure website without the need for separate data entries for each required data element at the website. The specific formats for the XML direct transfer may be downloaded from the website.

To fulfill this Army reporting requirement, the following GTL's information is provided:

The Unit Identification Code (UIC) for the Primary Government Task Leader is: _____

The Command Code for the Primary Government Task Leader is: _____

(The above will be provided during Contract Award)

5.8 Reserved

5.9 Work Site

The Contractor shall maintain work site and storage areas in accordance with local regulations and laws. Contractor personnel shall keep personal belongings to a minimum at all site locations. Contractor personnel shall not store documents that contain Personal Identifiable Information or HIPPA information unless the item containing the information was issued by the Government in support of this Task Order or is required to perform functions of this Task Order. Contractor personnel shall arrange personal belongings in a manner whereby they are easily identifiable and does not inter-mingle Government equipment or information (documents) with personal belongings or information. The Contractor shall ensure that all personnel remove personal items upon out-processing.

5.10 Changes to Operational Requirements

5.10.1. DoD Insourcing

In-sourcing is the conversion of currently contracted service to DOD civilian or military performance, or a combination of thereof. The Government will assess requirements to de-scope work on this Task Order to meet in-sourcing mandates based on changing DoD, Army

resource policies, or changing operational requirements, on as-needed basis. The Contractor shall be prepared to address decreased changes in work scope.

5.10.2. Changes to Operational Requirements

The Government will assess requirements to increase or modify the scope work on this Task Order to meet changes to DoD security strategy, resource policies, or operational requirements, on as-needed basis. The Contractor shall be prepared to address changes in work scope.

PART 6

APPLICABLE PUBLICATIONS

6. APPLICABLE PUBLICATIONS (CURRENT EDITIONS)

6.1. The Contractor shall abide by all applicable regulations, publications, manuals, and local policies and procedures.

The following documents are referenced for the performance of this effort:

The PWS may set a higher standard of performance than an applicable Army regulation. The PWS shall control over the regulations unless a particular PWS provision is in direct conflict with the applicable provision of the Army regulation. The COR will make this determination. Most publications may be downloaded from the Internet Web sites or may be ordered. The Government will provide those publications not available on a Web site or via mail order. The Contractor shall inform the COR of any change to a publication or document that affects the cost of the Task Order.

Army Information Technology Service Management (ITSM) Policy	http://ciog6.army.mil/Portals/1/Policy/2015/Army%20ITSM%20Policy_17Nov2014.pdf
AR 25-1, Army Information Management, 15 February 2000.	http://armypubs.army.mil/epubs/pdf/r25_1.pdf
AR 25-2, Information Assurance, 14 November 2003.	https://ia.signal.army.mil/docs/AR25_2.asp
AR 25-30, The Army Publishing and Printing Program, 26 March 2006.	http://www.apd.army.mil/pdffiles/r25_30.pdf
AR 25-50, Preparing and Managing Correspondence, 3 June 2002.	http://www.chapnet.army.mil/pdf/AR_25_50.pdf
AR 25-52, Authorized Abbreviations, Brevity Codes, and Acronyms, 4 January 2005.	http://www.apd.army.mil/pdffiles/r25_52.pdf
AR 190-13, The Army Physical Security Program.	AR 190-13, The Army Physical Security Program.
AR 190-16, Physical Security, 31 May 91.	http://www.apd.army.mil/jw2/xmldemo/r190_16/main.asp
AR 380-5, 29 September 2000, Department of the Army Information Security Program.	http://www.apd.army.mil/pdffiles/r380_5.pdf
AR 380-40, Policy for Safeguarding and Controlling Communications Security (COMSEC) Material, 7 September 2012.	https://armypubs.us.army.mil/epubs/DR_pubs/DR_b/pdf/r380_40.pdf
AR 380-67, DA Personnel Security	http://www.apd.army.mil/pdffiles/r380_67.pdf

Program, 9 September 1988.	
AR 381-14, Technical Counterintelligence (TCI), Headquarters Department of Army, 30 Sep 02 (C).	http://www.apd.army.mil/jw2/xmldemo/r381_12/head.asp
AR 530-1, Operations Security, 19 April 2007.	http://fas.org/irp/doddir/army/ar530-1.pdf
AR 602-2, Manpower and Personnel Integration (MANPRINT) in the System Acquisition Process, 1 June 2001.	http://www.apd.army.mil/pdffiles/r602_2.pdf
CJCSI 6510.06 (Series): "Communications Security Release to Foreign Nations."	Limited Access – Will be Provided Access during Phase-In Period
CJCSM 6510.01B, 10 July 2012, Cyber Incident Handling Program	http://dtic.mil/cjcs_directives/cdata/unlimit/m651001.pdf
CJCSI 6211.02D Defense Information System Network (DISN) Responsibilities. 01 January 2012	http://dtic.mil/cjcs_directives/cdata/unlimit/6211_02.pdf
CJCSM 6510.01A Information Assurance (IA) and Computer Network Defense (CND) Volume 1, Incident Handling Program, 24 June 2	http://dtic.mil/cjcs_directives/cdata/unlimit/6510_01.pdf
CJCSI 6510.01F Information Assurance (IA) and Support to Computer Network Defense (CND), 9 February 2011 *Directive current as of 10 October 2013*	http://dtic.mil/cjcs_directives/cdata/unlimit/6510_01.pdf
CONPLAN 5000 Series Military Concept Plans	Limited Access – Will be Provided Access during Phase-In Period
DOD 5220.22-M, National Industrial Security Program, Operating Manual, 28 February 2006.	http://www.dss.mil/documents/odaa/nispom2006-5220.pdf
DODD 5230.24, Distribution Statements on Technical Documents, 18 March 1987.	http://www.acqnotes.com/Attachments/DoD%20Directive%205230.24%20“Distribution%20Statements%20on%20Technical%20Documents”%2018%20March%201987.pdf
DOD 8510.01, DODI Risk Management Framework (RMF) for DoD Information Technology (IT) 12 March 2014.	http://dtic.mil/whs/directives/corres/pdf/851001_2014.pdf
DoDI 8500.1, Cybersecurity, 14 March 2014	http://dtic.mil/whs/directives/corres/pdf/850001_2014.pdf
DoD 8570.01-M Information Assurance Workforce Improvement Program. Incorporating change 3, January 24, 2012	http://dtic.mil/whs/directives/corres/pdf/857001m.pdf
DoD Architecture Framework	http://dodcio.defense.gov/TodayinCIO/DoDArchitectureFramework.aspx

DOD Policies and Plans on JIE	http://dodcio.defense.gov/Initiatives/JointInformationEnvironment.aspx
DOD Policies on Cloud Computing and Data Center Consolidation	http://dodcio.defense.gov/Portals/0/Documents/DoD%20Cloud%20Computing%20Strategy%20Final%20with%20Memo%20-%20July%205%202012.pdf
DOD Policies on Unified Communications	http://www.disa.mil/services/network-services/ucco
DoDI 8580.1, Information Assurance in the Defense Acquisition System, 9 July 2004	http://dtic.mil/whs/directives/corres/pdf/858001p.pdf
DoD 5105.21-M-1 Sensitive Compartmented Information Administrative Security Manual, dated 19 October 2012	http://dtic.mil/whs/directives/corres/pdf/510521m_vol2.pdf
DoD 5105.21-M-2 SCI SI Manual, dated 19 October 2012	http://dtic.mil/whs/directives/corres/pdf/510521m_vol1.pdf
DoD 5105.21-M-3 SCI TK Manual, dated 19 October 2012	http://dtic.mil/whs/directives/corres/pdf/510521m_vol1.pdf
DOD IT Standards Registry, (.mil/.gov only)	Limited Access – Will be Provided Access during Phase-In Period
DOD 5200.01, Vol 1-4, Department of Defense (DOD) Information Security Program, February 24, 2012	http://dtic.mil/whs/directives/corres/pdf/520001_vol1.pdf
DOD CIO Memo, Interim Department of Defense (DOD) Information Assurance (IA) Certification and Accreditation (C&A) Process Guidance, 6 July 2006	http://www.prim.osd.mil/Documents/Interim_DoD_IA_CA_ProcessGuidance.pdf
Directive-Type Memorandum (DTM) 08-003, "Next Generation Common Access Card (CAC) Implementation Guidance", 1December 2008, *Incorporating Change 5, 8 October 2013*	http://www.cac.mil/docs/DTM-08-003.pdf
DIACAP Frequently Asked Questions (FAQs), 18 July 2006	https://acc.dau.mil/adl/en-US/106876/file/23937/DIACAP%20FAQs%20071806.pdf
Existing and active USSOUTHCOM CONPLANs, FUNCPLANs, Operation Orders (OPORDs), and Execute Orders (EXORDs)	Limited Access – Will be Provided Access during Phase-In Period
E-Government Act of 2002 (Public Law 107-347)	http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf
Federal Information Security Management Act of 2002 (Title III of E-Gov)	http://csrc.nist.gov/drivers/documents/FISMA-final.pdf

JP 3-13 Joint Doctrine for Information Operations, dated 27 November 2012	http://dtic.mil/doctrine/new_pubs/jointpub_operations.htm
JP 3-13.3 Joint Publication for Operations Security (04 January 2012)	http://dtic.mil/doctrine/new_pubs/jointpub_operations.htm
JP 3-13.4 Joint Publication for Military Deception (26 January 2012)	http://dtic.mil/doctrine/new_pubs/jointpub_operations.htm
JP 3-54 Joint Doctrine for Operations Security, dated 24 January 1997	http://dtic.mil/doctrine/new_pubs/jointpub_operations.htm
JP 3-58 Joint Doctrine for Military Deception, dated 31 May 1996	http://dtic.mil/doctrine/new_pubs/jointpub_operations.htm
Memorandum, SAIS-IOM, Army Policy for use of the Army's Microsoft Enterprise License Agreement (ELA), 4 Feb 2004	http://www.thursby.com/sites/default/files/images/TECHCON%202003-005d%20Desktop%20STD%20-21Aug07.pdf
National Institute of Standards and Technology Special Publication 800-53A, "Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans," June 2010, as amended	http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf
National Institute of Standards and Technology Special Publication 800-39, "Managing Information Security Risk: Organization, Mission, and Information System View," March 2011	http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf
National Institute of Standards and Technology Special Publication 800-30, "Guide for Conducting Risk Assessments," September 2012, as amended	http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf
NSA/CSS Policy Manual 3-16: "Control of Communications Security (COMSEC) Material."	Limited Access – Will be Provided Access during Phase-In Period
NSTISSI No.7003, Protective Distribution Systems (PDS), 13 Dec 1996.	http://www.dss.mil/documents/odaa/protective_distribution_systems.pdf
NSTISSAM TEMPEST/2-95A, Red/Black Installation Guidance, Amendment, 3 February 2000.	Limited Access – Will be Provided Access during Phase-In Period
NSTISSI No.7003, Protective Distribution Systems (PDS), 13 Dec 1996	https://ia.signal.army.mil/docs/nstissi_7003.pdf
NSTISSAM TEMPEST/2-95A, Red/Black Installation Guidance, Amendment, 3 February 2000	Limited Access – Will be Provided Access during Phase-In Period

NSA/CSS Policy Manual 3-16: "Control of Communications Security (COMSEC) Material"	Limited Access – Will be Provided Access during Phase-In Period
NIST 800-37, Information Security, Guide For Applying Risk Management Framework to Federal Information Systems, February 2010	http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf
NIST 800-53, Information Security, Recommended Security Controls for Federal Information Systems and Organizations, August 2009, *Includes updates as of 01 May 201*	http://www.sandia.gov/fso/PDF/flowdown/sp800-53-rev3-final_updated-errata_05-01-2010.pdf
National Institute of Standards and Technology Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," current edition	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
Security Technical Implementation Guides (STIGs)	http://iase.disa.mil/stigs/
SIPRNET GIG Interconnection Approval Process (GIAP) Cross Domain Solution (CDS) Connection Requirements, July 2004.	Limited Access – Will be Provided Access during Phase-In Period
TB 380-41, 15 Mar 06, Procedures for Safeguarding, Accounting, and Supply Control of COMSEC Materiel	Limited Access – Will be Provided Access during Phase-In Period
Army Regulation 710-2 Inventory Management, Supply Policy Below the National Level	http://www.apd.army.mil/pdffiles/r710_2.pdf
Army Regulation-735-5 Property Accountability, Property Accountability Policies-	http://www.apd.army.mil/pdffiles/r735_5.pdf

PART 7

ATTACHMENT/TECHNICAL EXHIBIT LISTING

Note: Any technical information is provided for information purposes only and may not reflect the exact configuration of any item that is currently operational.

7. Attachment/Technical Exhibit List:

7.1. Attachment 1/Technical Exhibit 1 – Deliverable Requirements

7.2 Attachment 2/Technical Exhibit 2 – Historical Workload Data

7.3. Attachment 3/Technical Exhibit ——3 – Location of IT Environments or Support and Associated Contracts

7.4. Attachment 4/Technical Exhibit 4 – IT Infrastructure and Systems Identified in APMS

7.5. Attachment 5/Technical Exhibit 5 – Security Requirements by Functional Area and Clearance Certifications

7.6 Attachment 6/Technical Exhibit 6 – Networks and Systems Under This Effort

7.7 Attachment 7/Technical Exhibit 7 –Quality Assurance Surveillance Plan

7.8 Attachment 8/Technical Exhibit 8 - On-Site and On-Call Support Requirements

7.9 Attachment 9/Technical Exhibit 9 - Services by Location

7.10 Attachment 10/Technical Exhibit 10 - Maintained, Hosted, or Hoteled User Web Based or Command and Control Government Developed Applications

7.11 Attachment 11/Technical Exhibit 11 - JIE Technical Implementation Guidelines

7.12 Attachment 12/Technical Exhibit 12 - Key Personnel Responsibilities and Minimum Qualifications

7.13 Attachment 13/Technical Exhibit 13 - Functions Requiring Non-Disclosure Agreements

7.14 Attachment 14/Technical Exhibit 14 – Summary of PC, Servers and Applications on Servers By Location

7.15. Attachment 15/Technical Exhibit 15 – VSAT Systems and Locations

7.16. Attachment 16/Technical Exhibit 16 MNIS and CENTRIXS Locations

7.17. Attachment 17/Technical Exhibit 17 – Life Cycle Related Projects

7.18 Attachment 18/Technical Exhibit 18 - Life Cycle Related Projects

7.19 Attachment 19/Technical Exhibit 19 – Level 1 and Level 2 Information Assurance Accreditation Package Work

7.20 Attachment 20/Technical Exhibit 20– Maintained Software Applications

7.21 Attachment 21/Technical Exhibit 21 Organizational Background Information

7.22 Attachment 22/Technical Exhibit 22 – JTF-Bravo Unique Services

7.23 Attachment 23/Technical Exhibit 23 – JTF-GTMO Unique Services

7.24 Attachment 24/Technical Exhibit 24 – Software Engineering and Integration

7.25 Attachment 25/Technical Exhibit 25 – Defense Cyber Operations and NetOps Tool Sets

7.26 Attachment 26/Technical Exhibit 26 – Generic Network Diagram

~~7.27 Attachment 27/Technical Exhibit 27 – DD-254~~

7.27 - Attachment 27 /Technical Exhibit 27 – Performance Requirements Summary

7.28 Attachment 28/Technical Exhibit 28 – DD-254 – SEE SEPARATE FILE

PART 7 – ATTACHMENT 1 - TECHNICAL EXHIBIT 1 – Deliverable Requirements

Each deliverable contained in this matrix is critical to the successful performance and completion of this project. It is not a comprehensive list of all activities required. Contractor shall meet ALL requirements in the PWS to include activities not listed in this matrix. Note that all documents that are required in multi-stages (i.e. draft, then final) must be approved by the Government before proceeding to the next stage. The Government will accept or reject each document within 2 weeks of submission or notify the Contractor of additional time required. Contractor shall post all deliverables to the GFE SharePoint (or equivalent) portal.

NO.	NAME	DESCRIPTION	FORMAT	PWS REFERENCE(S)	REQUIRED DATE	IMPACT IF NOT RECEIVED OR APPROVED
1	Post Award Conference Review/Quad-Monthly Progress Briefing	The contractor shall provide briefings to include a schedule on near term activities. Updates to briefings will include any action items from prior meetings and are due one week after completion of meetings.	MS Power Point	1.6.9	First deliverable is due 1 Week after start of the first period of performance. Post Award Conference will be held 2 Weeks after start of first period of performance. Monthly Progress Briefings are due and an associated meeting will be held throughout the first four months of the start of the first period of performance. After this time, Quad-Monthly (Every 4 Months) Progress Reports will be due 1 week before Quad-Monthly Reviews.	Unsuccessful performance

NO.	NAME	DESCRIPTION	FORMAT	PWS REFERENCE(S)	REQUIRED DATE	IMPACT IF NOT RECEIVED OR APPROVED
2	Periodic Program Progress, Status and Management Report	This report provides an overview of projects, activities, and tasks accomplished within the last two months and those forecasted into the future. Projects, activities and tasks will include meetings, scheduled outages when known, or any efforts related to modifications to include life cycle updates or new capabilities. Also addressed will be past and future travel accomplished or planned to include a summary of transmitted visit certifications. The reports also include a schedule that identifies milestones for all projects, tasks, or activities.	MS Word for the Status. MS Project and PDF version of MS Project print-out for the Schedule.	1.6.9.1, 1.6.13.1, 4.2.1	Bi-Monthly after start of first period of performance.	Unsuccessful performance.

NO.	NAME	DESCRIPTION	FORMAT	PWS REFERENCE(S)	REQUIRED DATE	IMPACT IF NOT RECEIVED OR APPROVED
3	IT Life Cycle Implementation and Quality Control Plan (LCIQCP)	This plan outlines how the Contractor shall manage all efforts on this Task Order. The plan addresses staffing, staff training and certification, reporting of activities, accomplishment of administrative tasks, tracking and control of Government Furnished Equipment, and provides a high-level overview of major 5.1.X technical tasks identified in specific PWS paragraphs. The plan will contain separate attachments with resumes of key personnel and Non-Disclosure Agreements for those personnel that require them. All other plans are considered annexes to this file. All other deliverables (assessments, reports) will be discussed in this document.	MS Word.	Paragraphs 1.6.1, 1.6.7.1, 1.6.7.2, 1.6.7.3, 1.6.7.4, 1.6.8.1, 1.6.8.3, 1.6.8.4, 1.6.8.6, 1.6.8.6.1, 1.6.11, 1.6.13.1, 1.6.13.2, 1.6.16., 3.4, 3.4.1., 5.0 and all 5.1 subparagraphs as well as paragraphs 5.2.4 and 5.2.4.3.	Draft Plan is due with Proposal. Second draft is due 60 Days after start of first period of performance. Final plan is due 90 Days after assumption of responsibility of the JTF-Bravo effort. The contractor shall update the LCIQCP as required during future system upgrades or modifications to the scope of work.	Unsuccessful performance.
4	Contractor Travel Expense Estimate	This document identifies all estimates for future travel. The report will be aligned with the future Country Travel Expense Report.	MS Word, MS Excel	1.6.13	No later than 10 days before travel for routine requirements. No later than 24 hours after travel for priority requirements.	Unsuccessful performance.
5	Contractor Travel Expense Report	This document identifies all costs for recently accomplished travel. The report will be aligned with the previously submitted Country Travel Expense Estimate.	MS Word, MS Excel	1.6.13	No later than 15 days after completion of travel.	Unsuccessful performance.

NO.	NAME	DESCRIPTION	FORMAT	PWS REFERENCE(S)	REQUIRED DATE	IMPACT IF NOT RECEIVED OR APPROVED
6	Theater Country Clearance Request	This document outlines all requests for travel on an immediate or planned basis.	TBD	1.6.13.1	As required to meet maintenance objectives	Unsuccessful performance.
7	Future OCONUS Travel Reporting	This document identifies all personnel that will travel in the future and documents that required OCONUS Travel Training was accomplished. Report addresses the purpose of the travel, accomplishments, reportable items, and also certifies that any mandatory reporting to the Defense Security Service was accomplished.	MS Word, MS Excel	1.6.13.1	As required to meet maintenance objectives. No later than 30 days after completion of travel.	Unsuccessful performance.
8	Yearly Completed OCONUS Travel Report	This report details all overseas travel accomplished in the year and assures required training was accomplished.	MS Word or Excel	1.6.13.2	Once per year at end of POP.	Unsuccessful performance.
9	Government Furnished Equipment Property Book	This is a list of all Government Furnished Equipment.	Website with list or web enabled database.	3.4.2.	Updated weekly. Made available at any time.	Unsuccessful performance

NO.	NAME	DESCRIPTION	FORMAT	PWS REFERENCE(S)	REQUIRED DATE	IMPACT IF NOT RECEIVED OR APPROVED
10	Operations and Maintenance Phase-In and SIPRNET/NIPRNET Deprecation Plan	This document identifies the manpower (number of personnel and skill sets), process, activities, and timeline for phase-in and assumption of responsibilities related to Operations and Maintenance of all systems. The plan will address the site-by-site and system by system assumption of responsibilities in accordance with the phase-in dates. Any assumptions with respect to government support will be addressed. The draft plan addresses the phase-in of all sites and the deprecation (transition to a single network) of all non-SC HQ networks onto the SCHQ network in a sequential manor. The second draft will update assumptions and process from the first draft based on findings from the first and second phase-in periods. Subsequent updates are required during respective phase-in periods.	Word Document	5.1.1.1	Draft Plan is due with proposal. Updates are due every 90 days until collapse of all networks is complete.	Unsuccessful performance.

NO.	NAME	DESCRIPTION	FORMAT	PWS REFERENCE(S)	REQUIRED DATE	IMPACT IF NOT RECEIVED OR APPROVED
11	IT Service Corrective Action Planning	This document identifies any modifications required to meet the Minimum Performance Requirements of a given service or system. The document shall identify alternative changes to the Minimum Performance Requirements if the changes are not accomplished. Contractor will acknowledge no need for plan or updates if no corrective action is required.	Word Format	5.1.1.1.1	Draft Plan is due 30 Days after completion of phase-in of any given contractor requirement. Updates are due every 90 days until any approved required corrective actions are completed.	Unsuccessful performance
12	Task Discrepancy Report	This report identifies any material discrepancies or conflicting guidance between requirements documents or verbal direction.	MS Word	5.0	As required. Within one (1) business day	Performance notice to the contract file.

NO.	NAME	DESCRIPTION	FORMAT	PWS REFERENCE(S)	REQUIRED DATE	IMPACT IF NOT RECEIVED OR APPROVED
13	Joint Information Environment Transformation. Deliverables for: a. Data Center Consolidation Planning b. Software as a Service Transition Planning c. Active Directory Planning d. Identity and Access Management Planning e. Client Modernization Planning f. Single Security Architecture Planning g. Unified Capabilities Planning	The plan identifies methods and approaches to gather and document technical implementation requirements and if applicable a preliminary design, as well as, associated policies and recommended changes to life-cycle operations and maintenance processes associated with the specific JIE effort under assessment. The deliverables will account for all factors and actions identified in the corresponding Attachment 11 JIE technical guideline.	A combination of MS Word, PowerPoint, Visio, Excel	5.1.1.2 and sub paragraphs	Draft Plan for each JIE effort is due with proposal. Second Draft is due 45 days after initiation of each specific task and final on completion of task.	Unsuccessful performance.
14	New Communications Systems Capability Planning	The plan identifies technical requirements, a preliminary design, as well as, associated policies and recommended changes to life-cycle operations and maintenance processes associated with the implementation of a new service or capability. If required, the plan will include a facility site analysis.	A combination of MS Word, MS PowerPoint Visio, Excel	5.1.1.3 and subparagraphs	Draft Plan for each new capability effort is due within 45 days after initiation of each specific task and final on completion of task.	Unsuccessful performance.

NO.	NAME	DESCRIPTION	FORMAT	PWS REFERENCE(S)	REQUIRED DATE	IMPACT IF NOT RECEIVED OR APPROVED
15	New Software Application Plan, Design, Transition Document.	The plan identifies technical requirements, a preliminary design, workflow diagrams, rules, as well as, associated policies and recommended changes associated with the implementation of a new software application. The contractor shall identify the type of development process to be used.	A combinati on of MS Word, Visio, Excel	5.1.9.2 and sub-paragraphs	Draft Plan for each new software capability effort is due within 45 days after initiation of each specific task and final on completion of task. Design is due 45 days after plan approval. Final documentation prior to transition to operations.	Unsuccessful performance.
16	Design for Collapse of SIPRNET and NIPRNET Networks.	This document identifies any design changes collapse the SIPRNET and NIPRNET networks to include remotely manage all networks and services from USSOUTHCOM HQ.	Word Document	5.1.2.1.1	Draft designs are due 90 days after the approved planning documents. Final documents are due within 30 days of receipt of comments.	Unsuccessful performance.

NO.	NAME	DESCRIPTION	FORMAT	PWS REFERENCE(S)	REQUIRED DATE	IMPACT IF NOT RECEIVED OR APPROVED
17	Joint Information Environment Transformation Designs for: a. Data Center Consolidation Design b. Software as a Service Transition Design c. Active Directory Design d. Identity and Access Management Design e. Client Modernization Design f. Single Security Architecture Design g. Unified Capabilities Design	This deliverable contains a detailed Service Design Package which includes the following artifacts as appropriate: a) detailed architectures, b) drawings, c) equipment lists, d) process descriptions, e) policies and other appropriate documentation such as f) test plans, as well as, g) timelines, g) dependencies, h) assumptions, i) required manpower (by labor category and hours) in the transition phase, j) equipment, and k) circuits to meet current and future agreed mission requirements and associated life cycle sustainment efforts. Architecture products will be updates and adaptations to corresponding JIE Architecture Artifacts tailored to the SOUTHCOM environment.	A combination of MS Word, Visio, Excel	5.1.2.2. and sub paragraphs	Draft is due 60 days after initiation of each specific effort and final on completion of each effort. Final documents are due within 30 days of receipt of comments.	Unsuccessful performance.

NO.	NAME	DESCRIPTION	FORMAT	PWS REFERENCE(S)	REQUIRED DATE	IMPACT IF NOT RECEIVED OR APPROVED
18	New Communications Systems Design	This deliverable contains a detailed Service Design Package which includes the following artifacts as appropriate: a) detailed architectures, b) drawings, c) equipment lists, d) process descriptions, e) policies and other appropriate documentation such as f) test plans, as well as, g) timelines, g) dependencies, h) assumptions, i) required manpower (by labor category and hours) in the transition phase, j) equipment, and k) circuits to meet current and future agreed mission requirements and associated life cycle sustainment efforts.	A combinati on of MS Word, Visio, Excel	5.1.2.3 and sub paragraphs	Draft is due 60 days after initiation of each specific effort and final on completion of each effort. Final documents are due within 30 days of receipt of comments.	Unsuccessful performance.

NO.	NAME	DESCRIPTION	FORMAT	PWS REFERENCE(S)	REQUIRED DATE	IMPACT IF NOT RECEIVED OR APPROVED
19	Transition Documentation for Collapse of SIPRNET and NIPRNET Networks.	This deliverable contains all final changes implemented to remote manage all networks and services from SOUTHCOM HQ. The documents includes: a) test plans, procedures, and reports, b) as-built drawings, installation plans, interface control documents for data, power and cooling, and facility interface drawings, c) operations and maintenance instructions, d) user training plans and materials, e) new or updates to appropriate accreditation documents.	Word Document	5.1.3.1	Draft transition Documentation is required 90 days after approved design. Final documents are due within 30 days of receipt of comments.	Unsuccessful performance.

NO.	NAME	DESCRIPTION	FORMAT	PWS REFERENCE(S)	REQUIRED DATE	IMPACT IF NOT RECEIVED OR APPROVED
20	Joint Information Environment Transformation Transition Documentation for: a. Data Center Consolidation Transition b. Software as a Service Transition c. Active Directory Transition d. Identity and Access Management Transition e. Client Modernization Transition f. Single Security Architecture Transition g. Unified Capabilities Transition	This deliverable contains all final changes implemented to include: a) test plans, procedures, and reports, b) as-built drawings, installation plans, interface control documents for data, power and cooling, and facility interface drawings, c) operations and maintenance instructions, d) user training plans and materials, e) new or updates to appropriate accreditation documents..	A combination of MS Word, Visio, Excel	5.1.3.2. and all subparagraphs	Draft is due 60 days after initiation of each specific effort and final on completion of each effort. Final documents are due within 30 days of receipt of comments.	Unsuccessful performance.

NO.	NAME	DESCRIPTION	FORMAT	PWS REFERENCE(S)	REQUIRED DATE	IMPACT IF NOT RECEIVED OR APPROVED
21	New Communications Systems Capabilities Transition	This deliverable contains all final changes implemented to include: a) test plans, procedures, and reports, b) as-built drawings, installation plans, interface control documents for data, power and cooling, and facility interface drawings, c) operations and maintenance instructions, d) user training plans and materials, e) new or updates to appropriate accreditation documents.	A combinati on of MS Word, Visio, Excel	5.1.3.3	Draft is due within 60 days after initiation of each effort and final on completion of each effort. Final documents are due within 30 days of receipt of comments.	Unsuccessful performance.

NO.	NAME	DESCRIPTION	FORMAT	PWS REFERENCE(S)	REQUIRED DATE	IMPACT IF NOT RECEIVED OR APPROVED
22	Service Operations and Maintenance Plan	This plan addresses and synchronizes all the activities within paragraph 5.1.4 and associated sub-paragraphs. The plan outlines all the processes to be executed, which work centers will be involved, and identify specific position to include duty titles, skill sets, and experience required for accomplish the various aspects of accomplishing Service Operations and Maintenance. The plan will include a table of periodic processes to be accomplished and when the deliverables or statuses from those processes are due. The plan will identify linkages to IT Support Services such as Training, Configuration Management, Logistics, and Procurement. The plan also factors life-cycle support activities such as establishing and maintaining a spares pool for all critical equipment, critical components of critical equipment, life cycle replacement of all major components, and discussion on which maintenance processes will be out outsourced to consultants, OEM, or local vendors. Additionally, the plan shall identify major systems requiring consultants, OEM or OEM certified gold partner verification of configuration on a periodic basis. The Service Operations and Maintenance Plan contains an attachment identifying when all Hardware, as well as, User applications and infrastructure or platform software will be life cycled. This attachment will be synchronized with the Life Cycle Procurement Plan.	MS Word	5.1.4. and all sub-paragraphs.	Draft Plan is Due with Proposal. Updates are due every 90 days during the base period and then every 180 days during the option periods. Updates are required during future system upgrades or modifications to the scope of work.	Unsuccessful performance.

NO.	NAME	DESCRIPTION	FORMAT	PWS REFERENCE(S)	REQUIRED DATE	IMPACT IF NOT RECEIVED OR APPROVED
23	IT Service Catalog	This document/web site outlines all services available to Users, as well as, services used to operate and protect the network.	Web Site	5.1.4	Draft Catalog is due at the end of each phase-in period. Updates are due before transitioning new services to users.	Unsuccessful performance.
24	STIG and IVAM Impact Assessments	The assessment documents if STIG and IAVM mandates affect service availability or capabilities.	MS Word, and Active Web Page	5.1.4	Within 15 days of accomplishing STIG or IVAM implementation	Unsuccessful performance
25	Customer Portable Asset Tracking and Control List	The list contains the all portable assets and identifies assigned personnel.	Web based list.	5.1.4.2.7	60 Days after assumption of each site/contract and then updates monthly.	Unsuccessful performance
26	Script Management	The list contains all current scripts to include descriptions.	Web based list.	5.1.4.4.1.3	60 Days after assumption of each site/contract and then updates monthly.	Unsuccessful performance
27	Hoteled Systems List	The list identifies all hoteled systems by location and network.	Web based list	5.1.4.4.5.1	60 Days after assumption of each site/contract and then updates monthly.	Unsuccessful performance
28	Telephone Systems Directory	The directory contains a list of all telephone numbers and associated users or work centers.	Web based list.	5.1.4.4.9.3	60 Days after assumption of each site/contract and then updates bi-monthly.	Unsuccessful performance
29	IT System Usage Logs	The logs identify all IT systems used by any given User for the specified period.	MS Word or Excel	5.1.4.4.10	Within 15 days of request.	Unsuccessful performance
30	COMSEC Inventory Report	The list identifies all COMSEC and CCI to include hand receipt holders.	Web based list	5.1.10.1.2.1.12	15 Days after assumption of responsibilities for each site and then updates bi-monthly.	Unsuccessful performance

NO.	NAME	DESCRIPTION	FORMAT	PWS REFERENCE(S)	REQUIRED DATE	IMPACT IF NOT RECEIVED OR APPROVED
31	CSII Usage Report	The report contains User usage rates for CSII. The report includes username/nation, IP address accessed from, start/stop time and total time for system administrator during the specified period.	MS Word, MS Excel or Web Site	5.1.4.4.15.2	Reports are due monthly after assumption of responsibilities.	Unsuccessful performance
32	CSII Sensor Integration Checklist	The Checklist contains a CSII software suite troubleshooting flow chart to support O&M and PN training on user interface functions and related approved software applications.	MS Word	5.1.4.4.15.4	Checklist is due 60 days after assumption of responsibilities.	Unsuccessful performance
33	VSAT Survey Report	The report contains installation drawings for all VSAT locations. The report also contains requirements for authority to operate.	MS Word, MS Visio	5.1.4.4.12.2.2	Report is due 30 days after initiation of each effort.	Unsuccessful performance
34	Minimum Performance Requirements	Performance levels on a by system/service will be reported monthly for all locations. The report will include changes from the last 6 months for all systems and services.	MS Word and Live Web Site	5.1.5.	30 Days after Assumption of responsibilities of the first site. Monthly reporting thereafter.	Unsuccessful performance
35	Key Performance Indicators	Key performance indicators will be provided and reported. The report shall be on a by-network or by system basis if applicable.	MS Excel and Live Web Site	5.1.6 and all sub-paragraphs.	30 Days after Assumption of responsibilities of the first site. Monthly reporting thereafter.	Unsuccessful performance

NO.	NAME	DESCRIPTION	FORMAT	PWS REFERENCE(S)	REQUIRED DATE	IMPACT IF NOT RECEIVED OR APPROVED
36	Bandwidth Metrics	Bandwidth metrics for all NIPRNET, SIPRNET, JWICS and Satellite Circuits shall be provided. Bandwidth assessment of internal connectivity will also be reported.	MS Excel and Live Web Site	5.1.6.5	30 Days after Assumption of responsibilities of the first site. Monthly reporting thereafter.	Unsuccessful performance
37	TNCC COMSTAT Report	This report contains the status of all systems and networks in the AOR.	MS Word AND Live Web site.	5.1.7.2, 5.1.4.5	Daily after assumption of responsibilities.	Unsuccessful performance
38	Process Improvement Recommendations	The report contains an assessment and recommendations for improvements for processes, services, and system or network deficiencies.	MS Word	5.1.7	Yearly	Unsuccessful performance
39	Analysis of COMSTAT Network Service Call Report, Services Desk Reports and Logs	The report contains a monthly analysis of Communications Status (COMSTAT) Network Service Call Report, Service Desk Reports, Logs and KPIs.	MS Word	5.1.7.2	Monthly after assumption of responsibilities.	Unsuccessful performance
40	Quality Control Audit Report	The report contains results of self-audits against the LCIQCP. The report identifies all areas where the required quality is not met and uses this to execute corrective action steps.	MS Word.	5.1.7.1	Twice yearly.	Unsuccessful performance

NO.	NAME	DESCRIPTION	FORMAT	PWS REFERENCE(S)	REQUIRED DATE	IMPACT IF NOT RECEIVED OR APPROVED
41	IT Systems Support Services (ITSSS) – Bi-Weekly Accomplishment and Future Activities Status Report	This report identifies a) planned work per for the period, b) accomplished work for the period c) rationale for work not accomplished, d) planned work for the future on a per CME basis for each CME working on efforts related to paragraph 5.1.10 and below.	MS Word	5.1.10 and all sub-paragraphs	Every two weeks.	Unsuccessful performance
42	Investigation Reports	This report outlines the circumstances and findings of investigations by the contractor.	MS Word	1.6.7.4	Two weeks after request is made.	Unsuccessful performance
43	Training Material	This deliverable contains web based or document based training material.	Web based or document based.	5.1.10.2.1 and subparagraphs	Dependent of the magnitude of the effort. 60 Days for small efforts, 120 days for large efforts.	Unsuccessful performance
44	SEI Compliance Report	This report identifies test results delineating the SEI Policy Compliancy of applications	MS Word.	5.1.9.2.1	120 Days after assumption of responsibilities for SEI. Periodic updates as required.	Unsuccessful performance
45	List of Hosted Services	This Report contains a list of all current Hosted applications.	Live List (Web Site) and MS Word.	5.1.9.3	30 Days after assumption of responsibilities of each server farm.	Unsuccessful performance
46	Cyber Security Plan	This Report contains a plan which outlines how the contractor will ensure compliance with all Cyber Security requirements.	MS Word	5.1.10.1.2	Draft Plan Due as part of Proposal. 1st Update is 60 days after assumption of first site. Updates are due 30 days after assumptions of additional sites.	Unsuccessful performance

NO.	NAME	DESCRIPTION	FORMAT	PWS REFERENCE(S)	REQUIRED DATE	IMPACT IF NOT RECEIVED OR APPROVED
47	INFOCON, FRAGO, and CTO Compliance Report	This report contains an analysis of performance as well as an overview of compliance in Information Conditions (INFOCON) changes and Communications Tasking Orders (CTO).	MS Word, Active Web Page	5.1.10.1.2.1.1	Weekly updates after initial assumption of responsibilities.	Unsuccessful performance
48	STIG Analysis Report	The report contains an analysis of STIG as well an action plan including milestones due within required timeframes per DoDI 8510.01	MS Word, Active Web Page	5.1.10.1.2.1.2	Bi-Monthly Updates after initial assumption of responsibilities.	Unsuccessful performance
49	Cyber Readiness Report	The report addresses how the Contractor shall resolve open security vulnerabilities in a timely manner focusing on most critical vulnerabilities first.	MS Word, Active Web Page	5.1.10.1.2.1.3	Monthly Updates after initial assumption of responsibilities.	Unsuccessful performance
50	Vulnerability Scans Report	The report contains a log of all vulnerability scans and checks accomplished.	MS Word, Active Web Page	5.1.10.1.2.1.5	Monthly Updates after initial assumption of responsibilities.	Unsuccessful performance
51	Web Content Filter Report	This report contains a log of all web content filtering and monitoring collected to include prohibited web sites.	MS Word, Active Web Page	5.1.10.1.2.1.6	Within 24 hours of identification of incidents. Monthly summaries of incidents.	Unsuccessful performance
52	Information Assurance Tool Service Support	This report contains a log of activities and any findings.	MS Word, Active Web Page	5.1.10.1.2.1.7	Within 24 hours of identification of incidents. Monthly summaries of incidents.	Unsuccessful performance
53	Incidents Report	This report contains any incidents that are found or made aware to the contractor.	MS Word, Active Web Page	5.1.10.1.2.1.9	Within 24 hours of identification of incidents. Monthly summaries of incidents.	Unsuccessful performance

NO.	NAME	DESCRIPTION	FORMAT	PWS REFERENCE(S)	REQUIRED DATE	IMPACT IF NOT RECEIVED OR APPROVED
54	Network Security Event Log	This Report contains firewall logs, system logs, and associated media to designated organizations in the performance of forensic analysis services.	MS Word, Active Web Page	5.1.10.1.2.1.11	Within 24 hours of identification of incidents. Monthly summaries of incidents.	Unsuccessful performance
55	Reserved					
56	SharePoint Activities Report	The report contains a log of all SharePoint activities accomplished.	MS Word	5.1.10.2.6	Monthly after assumption of responsibilities.	Unsuccessful performance
57	Configuration Management Plan	The plan shall outline the tools, manpower, and activities that will be executed to ensure configuration management of all systems. The plan shall tie back to other activities to include capability integration and life cycle upgrades.	MS Word	5.1.10.1.3	Draft Plan Due as part of Proposal. Final plan is due 120 days after contract award.	Unsuccessful performance
58	Configuration Control and Change Board Report	This report contains a summary of all Configuration Control Board Approved Changes accomplished weekly.	MS Word	5.1.10.1.3.1	Weekly updates after initial assumption of responsibilities.	Unsuccessful performance
59	System Documentation – Approved Baselines and Installation Drawings	The approved baseline and installation drawing package shall include descriptions, lists, and drawings of all systems and networks.	MS Word, Excel, Visio, PowerPoi nt	5.1.10.1.3.2, 5.1.10.1.3.3	Prior to implementing any major modification or new system installation.	Unsuccessful performance

NO.	NAME	DESCRIPTION	FORMAT	PWS REFERENCE(S)	REQUIRED DATE	IMPACT IF NOT RECEIVED OR APPROVED
60	Physical Configuration Audit Reports	The report contains Physical Configuration Audits (PCAs) for each of the sites in the AOR.	MS Word	5.1.10.1.3.4	These reports are done on an annual basis at SCHQ, JTF-Bravo and JTF-GTMO.	Unsuccessful performance
61	Functional Configuration Verification and Audit Reports	This report contains an assessment of the functional configuration of all major modifications to systems or new system implementation. The report discusses the ability of systems to meet expected performance requirements.	MS Word	5.1.10.1.3.5	Prior to transition to operations for any major modification or new system implementation.	Unsuccessful performance
62	IT Hardware, Software, Warrantee, License, and Expendables Procurement Plan	This plan encompasses a life cycle procurement action that includes timing, volume, and cost estimates for life-cycle replacement and routine spare-parts provisioning of all hardware and software supported on this Task Order. The plan also includes timing and cost estimates for licenses and warranties.	MS Word	5.1.10.1.4.3	Draft as Part of Proposal. One update due 120 Days after contract award, Updates every 3 Months during the base period then every 6 months during the option periods.	Unsuccessful performance
63	Inventory of Spare Parts, Consumable, Material and Re-order Point Levels List	The list shall identify all recommended spares, consumables and Material Re-order point levels.	MS Excel	5.1.10.1.4.4	Draft Due 120 Days after assumption of responsibilities. Updates monthly.	Unsuccessful performance
64	Licenses and Warrantees List	This list contains all IT equipment licenses and warranties for AOR.	MS Excel	5.1.10.1.4.5	Draft Due 120 Days after assumption of responsibilities. Updates monthly.	Unsuccessful performance

NO.	NAME	DESCRIPTION	FORMAT	PWS REFERENCE(S)	REQUIRED DATE	IMPACT IF NOT RECEIVED OR APPROVED
65	JTF-GTMO Security Inspections	The report shall identify all accomplished security inspections.	MS Word	5.1.11.2	Monthly	Unsuccessful performance
66	Contingency Plan	This plan contains actions to allow for continued performance 24/7/365 in the event of catastrophic and non-catastrophic events and work stoppages.	MS Word	5.2.5.3	Draft Due 120 Days after contract award, Final within 90 Days after assumption of JTF-Bravo. Yearly Updates	Unsuccessful performance
67	Remote Site Recovery report	This report contains information addressing the results after each remote site recovery action.	MS Word	5.2.5.1	As Required - within 10 Days of Site Recovery - Summary Report Due within 1 Day	Unsuccessful performance
68	Failover Testing Report	This report contains the results of the failover testing of the internal backup systems to external replication sites. The report is submitted quarterly.	MS Word	5.2.5.2	As Required - within 10 Days of Complete of Testing	Unsuccessful performance
69	Internet Service Provider Requests	The document shall identify location, cost estimates, and purpose for ISP requests.	MS Word	5.3.1	As Required	Unsuccessful performance
70	OEM Support Services Report	The Report shall contain monthly hours or funds expenditures for all Consultants and OEM Support Services.	MS Word	5.1.10.3 and all sub-paragraphs	Monthly	Unsuccessful performance
71	Transportation Plan	The Transportation Plan shall identify the process to ship all IT equipment as required throughout the AOR or to Consultants or OEMs for corrective action.	MS Word	5.1.10.1.5.3	Draft plan is due 180 Days after start of first period of performance. Updates every 90 Days during the base period. Yearly updates are required thereafter.	Unsuccessful performance

NO.	NAME	DESCRIPTION	FORMAT	PWS REFERENCE(S)	REQUIRED DATE	IMPACT IF NOT RECEIVED OR APPROVED
72	Reserved					
73	Contractor Personnel Performing Work	The list shall contain the following information Full Name SSN Phone Number Email Address Name of Supervisor Phone Number of Supervisor Email Address of Supervisor Name of Company Indicator of Prime or Subcontractor Duty Title Assigned Work Center Duration of Assignment Date that JPAS visit certification was sent or date of local nation vetting completion.	MS Word or Excel and Live Web Site (Controlled Access SharePoint Site will be provided GFE)	4.2.2	At least 1 day prior to arrival at any location. Exceptions will be coordinated via Email with COR.	Denial of Access to any Facility
74	List of Required Common Access Cards and SIPRNET Tokens for Personnel Working on this Task Order	The Prime Contractor must provide and maintain a current list of all personnel (to include sub-contractor personnel) working on this Task Order that require Common Access Cards and SIPRENT Tokens.	MS Word or Excel and Live Web Site (Controlled Access SharePoint Site will be provided GFE)	4.8	At least 1 day prior to arrival at any location. Exceptions will be coordinated via email with the COR.	Denial of Access to any Facility or Network

NO.	NAME	DESCRIPTION	FORMAT	PWS REFERENCE(S)	REQUIRED DATE	IMPACT IF NOT RECEIVED OR APPROVED
75	Contractor Accomplished Required Training List	Contains a list of accomplished required training on a by person basis.	MS Word or Excel and Live Web Site (Controlled Access SharePoint Site will be provided GFE)	1.6.8.6	Within 2 weeks of any personnel arrival at any work site. Updated yearly.	Denial of Access to any Network
76	Non-Disclosure Agreements List	Prime contractor shall ensure appropriate personnel sign non-disclosure agreements	MS Word or and Live Web Site (Controlled Access SharePoint Site will be provided GFE)	1.6.16.1	Within 2 weeks of any personnel arrival at any work site. Updated yearly.	Denial of Access to work
77	DRMO Items	Log of all equipment or components turned-in to DRMO.	MS Work	3.4.5	15 days prior to sending items to DRMO.	Unsuccessful Performance
78	Funds Ledger and Computer Database	The ledger/data base tracks expenditures on this effort.	MS Excel and data base	PWS 5.1.0.1.1.2	Daily updates are due at the start of the first period of performance	Unsuccessful Performance
79	Logistics Support Plan	The plan identifies the processes and means to transport items.	MS Word	5.1.10.1.5	Draft plan is due within 90 days of start the first period of performance. Updates every 90 days during the base period and yearly thereafter.	Unsuccessful Performance

NO.	NAME	DESCRIPTION	FORMAT	PWS REFERENCE(S)	REQUIRED DATE	IMPACT IF NOT RECEIVED OR APPROVED
80	Reserved					
81	Reserved					
82	Reserved					
83	On – Call Report	The report contains daily and consolidated quarterly on-call response/incident report that shall include the following data fields: Date, Technician Called, Time of Initial Call, Time of Technician Arrival, Brief Problem Description, and Time of Resolution.	MS Word	5.2.3	As required and quarterly summary.	Unsuccessful Performance
84	Meeting/Conference Trip Report	The report shall contain the purpose and summary discussions of activities that occurred in meetings and conferences	MS Word	5.6	As required.	Unsuccessful Performance
85	Cyber Network Attack Investigation Report	The report contains discussion of activities accomplished under a cyber-attack.	MS Word, Active Web Page	5.1.10.1.2.1.10	As required – within 24 hours of attack and updated daily until event is complete.	Unsuccessful Performance
86	Reserved					
87	Reserved					

NO.	NAME	DESCRIPTION	FORMAT	PWS REFERENCE(S)	REQUIRED DATE	IMPACT IF NOT RECEIVED OR APPROVED
89	Design for SIPRNET and NIPRNET Collapse	This deliverable contains a detailed Service Design Package which includes the following artifacts as appropriate: a) detailed architectures, b) drawings, c) equipment lists, d) process descriptions, e) policies and other appropriate documentation such as f) test plans, as well as, g) timelines, g) dependencies, h) assumptions, i) required manpower (by labor category and hours) in the transition phase, j) equipment, and k) circuits to meet current and future agreed mission requirements and associated SIPRNET and NIPRNET collapse .	A combinati on of MS Word, Visio, Excel	5.1.2.1	Draft design is due 60 days after approval of plan and final 30 days after receipt of comments.	Unsuccessful performance.

NO.	NAME	DESCRIPTION	FORMAT	PWS REFERENCE(S)	REQUIRED DATE	IMPACT IF NOT RECEIVED OR APPROVED
90	Transition Package for SIPRNET and NIPRNET Collapse	This deliverable contains all final changes implemented to include: a) test plans, procedures, and reports, b) as-built drawings, installation plans, interface control documents for data, power and cooling, and facility interface drawings, c) operations and maintenance instructions, d) user training plans and materials, e) new or updates to appropriate accreditation documents.	A combinati on of MS Word, Visio, Excel	5.1.3.1.	Draft transition package is due 60 days after initiation of each specific tasks and final 30 days after receipt of comments.	Unsuccessful performance.
91	Software Engineering and Integration Activity Prioritization Report	The report shall contain a list of requested SEI activities to include estimated levels of manpower resource to complete efforts.	MS Word and a Live web site.	5.1.9.	Quarterly	Unsuccessful performance
92	Reserved					
93	Integrated Master Schedule	The document contains a list of all known activities and deliverables to be accomplished over at least a 2 year period	MS Project	5.1.10.1.1.3	Draft with proposal. Updates Monthly.	Unsuccessful performance

NO.	NAME	DESCRIPTION	FORMAT	PWS REFERENCE(S)	REQUIRED DATE	IMPACT IF NOT RECEIVED OR APPROVED
94	Reserved					
95	Reserved					
96	Cyber Incident Forensic Analysis Report	This report contains the results of reverse engineering anomalous / malicious software to identify root-cause issues that require mitigation. The report addresses preservation, identification, documentation, and interpretation of data on network and hard drives.	MS Word	5.1.10.1.2.1.10 .1	Draft report within 24 hours of identification of a malicious activity. Updates weekly until complete for each activity	Unsuccessful performance
97	JDIMS Training Plan	The JDIMS training Plan identifies training method(s), approach(s), frequency, proficiency level measurement, objectives, and assessment standard for use of the JDIMS application	MS Word	Attachment 5.7.1	The draft training plan shall be submitted within 30 days after assumption of JTF-GTMO responsibilities. The final training plan shall be submitted within five (5) working days of Government Comments. Updates are required after changes to the application that affect the User interface.	Unsuccessful performance
98	Reserved					
99	Required Training and Certifications	The report contains required training and certifications on a by-system and by-personnel basis.	MS Word, Active Web Page	1.6.8.3	Draft is due within 30day of assumption of responsibilities for any environment or system. Updates are due monthly.	Unsuccessful performance
100	Accreditation Packages Updates and Schedule	Each package is maintained in accordance with DoD instructions. The schedule provides visibility of when updates are due.	MS Office products.	5.1.10.1.2.1.14	Updates in accordance with DoD instructions	Unsuccessful performance

(b)(3):10 U.S.C. § 130,(b)(7)(E)

(b)(3):10 U.S.C. § 130,(b)(7)(E)

PART 7 – ATTACHMENT 3 - TECHNICAL EXHIBIT 3 - Location of IT Environments or Support and Associated Contracts

(b)(3): 10 U.S.C. § 130,(b)(7)(E)

(b)(3):10 U.S.C. § 130,(b)(7)(E)

(b)(3):10 U.S.C. § 130,(b)(7)(E)

(b)(3):10 U.S.C. § 130,(b)(7)(E)

(b)(3):10 U.S.C. § 130,(b)(7)(E)

(b)(3):10 U.S.C. § 130,(b)(7)(E)

(b)(3):10 U.S.C. § 130,(b)(7)(E)

(b)(3):10 U.S.C. § 130,(b)(7)(E)

(b)(3):10 U.S.C. § 130,(b)(7)(E)

(b)(3):10 U.S.C. § 130,(b)(7)(E)

DRAFT

QUALITY ASSURANCE SURVEILLANCE PLAN (QASP)

FOR

U.S. SOUTHERN COMMAND (USSOUTHCOM)

ENTERPRISE INFORMATION TECHNOLOGY SERVICES SUPPORT CONTRACT

(EITSSC)

Issued [Insert Date]

TABLE OF CONTENTS

1	INTRODUCTION	1
1.1	Purpose.....	1
1.2	Performance Management Approach	1
1.3	Performance Management Strategy	1
2	ROLES AND RESPONSIBILITIES	2
2.1	The Contracting Officer	2
2.2	The Contracting Officer's Technical Representative	2
3	IDENTIFICATION OF REQUIRED PERFORMANCE STANDARDS/QUALITY LEVELS	2
4	METHODOLOGIES TO MONITOR PERFORMANCE	2
4.1	Surveillance Techniques	2
4.2	Customer Feedback	3
4.3	Acceptable Quality Levels	3
5	QUALITY ASSURANCE DOCUMENTATION	3
5.1	The Performance Management Feedback Loop	3
5.2	Monitoring Forms	3
6	ANALYSIS OF QUALITY ASSURANCE ASSESSMENT	4
6.1	Determining Performance	4
6.2	Reporting.....	4
6.3	Reviews and Resolution	4
ATTAHCMENT 7 - APPENDIX 1: PERFORMANCE REQUIREMENTS SUMMARY		5
ATTACHMENT 7 - APPENDIX 2: SAMPLE QUALITY ASSURANCE MONITORING FORM		6

QUALITY ASSURANCE SURVEILLANCE PLAN (QASP)

1. INTRODUCTION

This quality assurance surveillance plan (QASP) is pursuant to the requirements listed in the performance work statement (PWS) entitled U.S. SOUTHERN COMMAND (USSOUTHCOM) ENTERPRISE INFORMATION TECHNOLOGY SERVICES SUPPORT CONTRACT (EITSSC). This plan sets forth the procedures and guidelines USSOUTHCOM J6 will use in ensuring the required performance standards or services levels are achieved by the contractor.

1.1 Purpose

The purpose of the QASP is to describe the systematic methods used to monitor performance and to identify the required documentation and the resources to be employed. The QASP provides a means for evaluating whether the contractor is meeting the performance standards/quality levels identified in the PWS and the contractor's quality control plan (QCP), and to ensure that the government pays only for the level of services received.

This QASP defines the roles and responsibilities of all members of the integrated project team (IPT), identifies the performance objectives, defines the methodologies used to monitor and evaluate the contractor's performance, describes quality assurance documentation requirements, and describes the analysis of quality assurance monitoring results.

1.2 Performance Management Approach

The PWS structures the acquisition around "what" service or quality level is required, as opposed to "how" the contractor should perform the work (i.e., results, not compliance). This QASP will define the performance management approach taken by USSOUTHCOM J6 to monitor and manage the contractor's performance to ensure the expected outcomes or performance objectives communicated in the PWS are achieved. Performance management rests on developing a capability to review and analyze information generated through performance assessment. The ability to make decisions based on the analysis of performance data is the cornerstone of performance management; this analysis yields information that indicates whether expected outcomes for the project are being achieved by the contractor.

Performance management represents a significant shift from the more traditional quality assurance (QA) concepts in several ways. Performance management focuses on assessing whether outcomes are being achieved and to what extent. This approach migrates away from scrutiny of compliance with the processes and practices used to achieve the outcome. A performance-based approach enables the contractor to play a large role in how the work is performed, as long as the proposed processes are within the stated constraints. The only exceptions to process reviews are those required by law (federal, state, and local) and compelling business situations, such as safety and health. A "results" focus provides the contractor flexibility to continuously improve and innovate over the course of the contract as

long as the critical outcomes expected are being achieved and/or the desired performance levels are being met.

1.3 Performance Management Strategy

The contractor is responsible for the quality of all work performed. The contractor measures that quality through the contractor's own quality control (QC) program. QC is work output, not workers, and therefore includes all work performed under this Task Order regardless of whether the work is performed by contractor personnel or by subcontractors. The contractor's QCP will set forth the staffing and procedures for self-inspecting the quality, timeliness, responsiveness, customer satisfaction, and other performance requirements in the PWS. The contractor will develop and implement a performance management system with processes to assess and report its performance to the designated government representative. The contractor's QCP will set forth the staffing and procedures for self-inspecting the quality, timeliness, responsiveness, customer satisfaction, and other performance requirements in the PWS. This QASP enables the government to take advantage of the contractor's QC program.

The government representative(s) will monitor performance and review performance reports furnished by the contractor to determine how the contractor is performing against communicated performance objectives. The government will make determination regarding incentives based on performance measurement metric data and notify the contractor of those decisions. The contractor will be responsible for making required changes in processes and practices to ensure performance is managed effectively.

2 ROLES AND RESPONSIBILITIES

2.1 The Contracting Officer

The contracting officer (CO) is responsible for monitoring contract compliance, contract administration, and cost control and for resolving any differences between the observations documented by contracting officer's representative (COR) and the contractor. The CO will designate one full-time COR, as the government authority for performance management. The number of additional representatives serving as technical inspectors depends on the complexity of the services measured, as well as the contractor's performance, and must be identified and designated by the CO.

2.2 The Contracting Officer's Representative

The contracting officer's representative (COR) is designated in writing by the CO to act as his or her authorized representative to assist in administering a contract. COR limitations are contained in the written appointment letter. The COR is responsible for technical administration of the project and ensures proper government surveillance of the contractor's performance. The COR is not empowered to make any contractual commitments or to authorize any contractual changes on the government's behalf. Any changes that the contractor deems may affect contract price, terms, or conditions shall be referred to the CO for action. The COTR will have the responsibility for completing QA monitoring forms used to document the inspection and

evaluation of the contractor's work performance. Government surveillance may occur under the inspection of services clause for any service relating to the contract.

2.3 The Assistant Contracting Officer's Representative

Due to the diversity of services on this Task Order, the Government shall assign multiple ACORs supporting the requirements of each major installation or program technical/functional area. The ACOR titles are identified below. ACORs monitor technical and functional aspects of the contract on a theater wide basis, as well as, administrative aspects of the contract on a regional basis. The ACORs are authorized to perform the following functions within their functional or technical area on behalf of the COR:

a. Assure that the Contractor performs the technical and administrative requirements of the contract
b. Perform inspections necessary in connection with Contractor performance
c. Maintain written and oral communications with The Contractor concerning technical aspects of the contract
d. Issue written interpretations of technical requirements, including Government drawings, designs, and specifications
e. Monitor Contractor's performance and notify both the COR and Contractor of any deficiencies

A letter of designation will be issued to each ACOR, a copy of which is sent to the Contractor, states the responsibilities and limitations of the respective ACOR, especially with regard to changes in cost or price, estimates or changes in delivery dates. ACORs are not authorized to change any of the terms and conditions of the resulting order.

2.4 The Assistant Contracting Officer's Representative by Technical or Functional Area

a. SCHQ IT Service Operations ACOR
b. JTF-Bravo IT Service Operations ACOR
c. JTF-GTMO IT Service Operations ACOR
d. SCO IT Service Operations ACOR
e. MNIS Service Operations ACOR
f. Enterprise Service Strategy, Design, and Transition ACOR
g. Continual Service Improvement ACOR
h. Enterprise Cyber Security Operations and Information Assurance ACOR
i. Enterprise Software Engineering and Integration/Application Development and Operations ACOR
j. Enterprise Unified Capabilities (Network Systems and Services) ACOR
k. Enterprise Data Center, Servers, and Storage ACOR
l. Enterprise Assistance and Advisory Services ACOR
m. Enterprise Cable Plant, LMR, Microwave and SATCOM ACOR
n. Enterprise Configuration Management ACOR
o. Enterprise Logistics Support ACOR
p. Microsoft Enterprise Project Management ACOR

3 IDENTIFICATION OF REQUIRED PERFORMANCE STANDARDS/QUALITY LEVELS

The required performance standards and/or quality levels are included in the PWS and in Attachment 1, “Performance Requirements Summary.” If the contractor meets the required service or performance level, it will be paid the monthly amount agreed on in the contract. Failure to meet the required service or performance level will result in a deduction from the monthly amount.

4 METHODOLOGIES TO MONITOR PERFORMANCE

4.1 Surveillance Techniques

In an effort to minimize the performance management burden, simplified surveillance methods shall be used by the government to evaluate contractor performance when appropriate. The primary methods of surveillance are (include those that apply)

Random monitoring, which shall be performed by the COR/ACOR designated inspector.

100% Inspection – Each month, the COR/ACOR, shall review the generated documentation and enter summary results into the Surveillance Activity Checklist.

Periodic Inspection – COR/ACOR typically performs the periodic inspection on a monthly basis.

4.2 Customer Feedback

The contractor is expected to establish and maintain professional communication between its personnel and customers. The primary objective of this communication is customer satisfaction. Customer satisfaction is the most significant external indicator of the success and effectiveness of all services provided and can be measured through customer complaints.

Performance management drives the contractor to be customer focused through initially and internally addressing customer complaints and investigating the issues and/or problems. The customer always has the option to communicate complaints to the COR or ACOR, as opposed to the contractor.

Customer complaints, to be considered valid, must set forth clearly and in writing the detailed nature of the complaint, must be signed, and must be forwarded to the COTR/COR. The COTR/COR will accept those customer complaints and investigate using the Quality Assurance Monitoring Form – Customer Complaint Investigation, identified in Appendix 3.

Customer feedback may also be obtained either from the results of formal customer satisfaction surveys or from random customer complaints.

4.3 Acceptable Performance Levels

The acceptable performance levels included in Appendix 1, Performance Requirements Summary Table, for contractor performance are structured to allow the contractor to manage how the work is performed while providing negative incentives for performance shortfalls.

5. QUALITY ASSURANCE DOCUMENTATION

5.1 The Performance Management Feedback Loop

The performance management feedback loop begins with the communication of expected outcomes. Performance standards are expressed in the PWS and are assessed using the performance monitoring techniques shown in Attachment 1.

5.2 Monitoring Forms

The government's QA surveillance, accomplished by the COR/ACOR, will be reported using the monitoring forms in Attachments 2 and 3. The forms, when completed, will document the government's assessment of the contractor's performance under the contract to ensure that the required service levels are being achieved.

The COR will retain a copy of all completed QA surveillance forms.

6 ANALYSIS OF QUALITY ASSURANCE ASSESSMENT

6.1 Determining Performance

Government shall use the monitoring methods cited to determine whether the performance standards/service levels/AQLs have been met. If the contractor has not met the minimum requirements, it may be asked to develop a corrective action plan to show how and by what date it intends to bring performance up to the required levels.

6.2 Reporting

At the end of each month, the COR will prepare a written report for the ACO summarizing the overall results of the quality assurance surveillance of the contractor's performance. This written report, which includes the contractor's submitted monthly report and the completed quality assurance monitoring forms (Attachment 2), will become part of the QA documentation. It will enable the government to demonstrate whether the contractor is meeting the stated objectives and/or performance standards, including cost/technical/scheduling objectives.

6.3 Reviews and Resolution

The COR required the contractor's project manager, or a designated alternate, to meet with the COR or ACOR and other government personnel as deemed necessary to discuss performance evaluation. The COR will define a frequency of in-depth reviews with the contractor, including appropriate self-assessments by the contractor; however, if the need arises, the contractor will meet with the COR or appropriate ACOR as often as required or per the contractor's request. The agenda of the reviews may include:

a. Monthly performance assessment data and trend analysis
b. Issues and concerns of both parties
c. Projected outlook for upcoming months and progress against expected trends, including a corrective action plan analysis
d. Recommendations for improved efficiency and/or effectiveness
e. Issues arising from KPI or Minimum Performance Requirements reporting

The COR must coordinate and communicate with the Contractor to resolve issues and concerns regarding marginal or unacceptable performance.

The COR and the Contractor should jointly formulate tactical and long-term courses of action. Decisions regarding changes to metrics, thresholds, or service levels should be clearly documented. Changes to service levels, procedures, and metrics will be incorporated as a contract modification at the convenience of the PCO/ACO.

APPENDIX 1: PERFORMANCE REQUIREMENTS SUMMARY

The Contractor Performance requirements are summarized into performance objectives that relate directly to mission essential items. The performance threshold briefly describes the minimum acceptable levels of service required for each requirement. These thresholds are critical to mission success. Task Order surveillance will be performed by the COR and appropriate ACORS.

Performance Objectives	Performance Standards	Performance Threshold	Methods of Surveillance	Impact on Contractor Payments or Other Impact
PRS #1 Accomplishment of Planning, Designing, Phase – In of work responsibilities or Transition New Technical/Operational Capabilities References: IT Service Strategy, (PWS 5.1.1) IT Service Design (PWS 5.1.2) IT Service Transition (PWS 5.1.3)	Technical performance. Meet the approved technical requirements, technical design and technical performance. Schedule. Meet the approved capability delivery schedules (Applies to JIE or New Capability CLINs) Timeliness of deliverables. Provide required documentation and reports in accordance with schedules. Resource control and Management. Meet milestones or complete deliveries within approved labor hours and labor costs. (Time and Materials CLINs Only)	For New/Modified Capabilities, Passes Acceptance Testing and conforms to Functional and Physical Configuration Audits. Within +/- 15% of the agreed schedule Within +/- 15% of the agreed schedule Within +/- 10% of agreed resources (labor hours or labor costs for Time and Material	100% Review of Deliverables	Positive Comments and Ratings or Negative comment and ratings respectively for successful or unsuccessful performance. Possible exercise of options for successful performance. Possible decision to not exercise future options for unsuccessful performance.

		CLINs)		
PRS #2 Meet Performance Requirements for All Services References IT Service Operations (PWS 5.1.4)	Meet performance requirements for all services identified in attachment 9 Timeliness of deliverables. Provide required documentation and reports in accordance with schedules.	Availability in accordance with attachment 9 Within +/- 15% of the agreed schedule	100% Review of Deliverables	Positive Comments and Ratings or Negative comment and ratings respectively for successful or unsuccessful performance. Possible exercise of options for successful performance. Possible decision to not exercise future options for unsuccessful performance.

PRS #3 Ability to Identify Process Improvements or Efficiencies Reference: Continuous IT Service Improvement (PWS 5.1.7)	Timeliness of deliverables. Provide required documentation and reports in accordance with schedules.	Within +/- 15% of the agreed schedule	100% Review of Deliverables	Positive Comments and Ratings or Negative comment and ratings respectively for successful or unsuccessful performance. Possible exercise of options for successful performance. Possible decision to not exercise future options for unsuccessful performance.
PRS #4 Accomplish Software Engineering and Integration Activities Reference Software Engineering Integration Life Cycle Support Activities (PWS 5.1.9)	Technical performance. Meet the approved technical requirements, technical design and technical performance. Schedule. Meet the approved capability delivery schedules (Applies to JIE or New Capability CLINs) Timeliness of deliverables. Provide required documentation and reports in accordance with schedules. Resource control and Management. Meet milestones or complete deliveries within approved	For SEI Capabilities, Passes Acceptance Testing and conforms to Functional and Physical Configuration Audits. Within +/- 15% of the agreed schedule Within +/- 15% of the agreed schedule Within +/- 10% of	100% Review of Deliverables	Positive Comments and Ratings or Negative comment and ratings respectively for successful or unsuccessful performance. Possible exercise of options for successful performance. Possible decision to not exercise future options for unsuccessful performance.

	labor hours and labor costs. (Time and Materials CLINs Only)	agreed resources (labor hours or labor costs for Time and Material CLINs)		
PRS #5 Accomplish IT Systems Support Services Reference: IT Systems Support Services (PWS 5.1.10)	Timeliness of deliverables. Provide required documentation and reports in accordance with schedules.	Within +/- 15% of the agreed schedule	100% Review of Deliverables	Positive Comments and Ratings or Negative comment and ratings respectively for successful or unsuccessful performance. Possible exercise of options for successful performance. Possible decision to not exercise future options for unsuccessful performance.
PRS #6 Accomplish Other Required Support Services in Colombia, JTF-Bravo, and JTF-GTMO Reference: Other Required Support Colombia, (JTF-Bravo, JTF-GTMO) (PWS 5.1.11)	Timeliness of deliverables. Provide required documentation and reports in accordance with schedules.	Within +/- 15% of the agreed schedule	100% Review of Deliverables	Positive Comments and Ratings or Negative comment and ratings respectively for successful or unsuccessful performance. Possible exercise of options for successful performance. Possible decision to not exercise future options for unsuccessful performance.

PRS #7 Accomplish Exercise and Contingency Operations Support Reference: Exercise and Contingency Operations Support PWS Paragraph 5.2.5	Timeliness of deliverables. Provide required documentation and reports in accordance with schedules.	Within +/- 15% of the agreed schedule	100% Review of Deliverables	Positive Comments and Ratings or Negative comment and ratings respectively for successful or unsuccessful performance. Possible exercise of options for successful performance. Possible decision to not exercise future options for unsuccessful performance.

ATTACHMENT 7 - APPENDIX 2: SAMPLE QUALITY ASSURANCE MONITORING FORM

SERVICE or STANDARD: _____

_____

_____

_____

_____

SURVEY PERIOD: _____

SURVEILLANCE METHOD (Check):

❒ Random Sampling ❒ 100% Inspection ❒ Periodic Inspection ❒ Customer Complaint

LEVEL OF SURVEILLANCE (Check):

❒ Monthly ❒ Quarterly ❒ As needed

PERCENTAGE OF ITEMS SAMPLED DURING SURVEY PERIOD: _____ %

ANALYSIS OF RESULTS:

Observed Service Provider Performance Measurement Rate: _____%

Service Provider's Performance (Check): ❒ Meets Standards

❒ Does Not Meet Standards

Narrative of Performance During Survey Period: _____

_____

_____

_____

_____

PREPARED BY: _____ **DATE:** _____

ATTACHMENT 7 - APPENDIX 3 CUSTOMER COMPLAINT INVESTIGATON FORM

TO BE DEVELOPED JOINTLY BY AWARDEE AND GOVERNMENT AFTER CONTRACT AWARD

PART 7 – ATTACHMENT 8 - TECHNICAL EXHIBIT 8 - On-Site and On-Call Support Requirements

Location	
USSC HQ 9301 NW 33rd Street, Doral FL, 33028	On-Site
Flag Officer Residences in the Miami Area. These are not identified in this document for security and privacy act reasons.	Off-Site
SOUTHCOM Washington Office (SCWO), Pentagon, Washington, DC	On-Site
DISA DECC San Antonio (On-Call/TDY as needed)	Off-Site
USSOUTHCOM DOS Certified theater warehouse – to be provided by Contractor	On-Site
Colombia, Bogota - American Embassy	On-Site
Brazil, Brasilia - American Embassy	On-Site
Barbados, Bridgetown	Off-Site
Peru, Lima – American Embassy	On-Site
Jamaica, Bridgetown - American Embassy	Off-Site
Argentina, Buenos Aires - American Embassy	Off-Site
Colombia, Cartagena - American Embassy	On-Site
Honduras, Tegucigalpa, American Embassy	On-Site
Belize, Belmopan - American Embassy	On-Site
El Salvador, San Salvador - American Embassy	On-Site
Guyana, Georgetown - American Embassy	Off-Site
Guatemala, Guatemala City - American Embassy	On-Site
Jamaica, Kingston - American Embassy	Off-Site
Nicaragua, Managua - American Embassy	On-Site
Guatemala, Monterrico - American Embassy	On-Site
Uruguay, Ciudad de la Costa - American Embassy	Off-Site
Panama, Panama City - American Embassy	On-Site
Suriname, Paramaribo - American Embassy	Off-Site
Paraguay, Asunción - American Embassy	Off-Site
Haiti, Port-au-Prince - American Embassy	Off-Site
Ecuador, Quito - American Embassy	Off-Site
Costa Rica, San Jose - American Embassy	On-Site
Chile, Santiago - American Embassy	On-Site
Dominican Republic, Santo Domingo - American Embassy	On-Site
Bolivia, La Paz - American Embassy	Off-Site
Trinidad and Tobago, Port of Spain	Off-Site
JIATF-South NAS Key West, FL Truman Annex	On-Site* (User Support Only)
US Navy South, Mayport FL	On-Site* (User Support Only)
Several Partner Nation Command Centers throughout the AOR	Off-Site

Joint Task Force Bravo, Soto Cano Air Base Honduras	On-Site
Radio/microwave tower sites near Soto Cano Air Base Honduras	Off-Site
Joint Task Force Guantanamo, Guantanamo Bay Cuba	On-Site
Brandy Station, VA (VSAT Hub)	Off-Site
All other VSAT locations per attachment 15	Off-Site
All MNIS locations per Attachment 16	Off-Site

(b)(3):10 U.S.C. § 130,(b)(7)(E)

PART 7 – ATTACHMENT 10 - TECHNICAL EXHIBIT 10 - Maintained, Hosted, or Hoteled User Web Based or Command and Control Government Developed Applications

Hosted means that the application is under the configuration control of an outside agency but runs on a physical or virtual server environment maintained by this effort.

Maintained means that the applications is under the development, configuration control and change management process of this effort.

Hoteled means that the only support provided is space, power, cooling, and Domain Name Service and Identity Access Management (IdAM)

All Hosted or Maintained application are .net based applications running on Windows based Servers with SQL Server provisioned databases.

SC HQ Hosted and Maintained Software Applications

Joint Award Submission	Maintained
Command Operational Readiness Tool	Maintained
SOUTHCOM Enterprise Management System (Human Resource Managements/Security Management/Network Access Management)	Maintained
Command Training Applications	Maintained
External User Registration System	Maintained
Resource Information Management System (RIMS)	Hosted
Tasker System	Hosted
Conference Room Schedule	Hosted
A/O of the Month Request	Hosted
Peer Recognition Program Tool	Hosted
Chief of Staff Kneeboard	Hosted
Command Calendar	Hosted
SCO Reporting/Director Weekly Reporting Tool	Hosted
Commanders Knowledge Wall	Hosted
CCA Kiosk	Hosted
TV Announcements	Hosted
Career Planning/Mentoring Tool	Hosted
Civilian Evaluation (TAPES)	Hosted
Theater Security Cooperation Management System (TSCMIS)	Hosted
SC TCA Information Management System (SCTIMS)	Hosted
Americas Network (AMNET)	Hosted
Strategic Assessment Tool	Hosted
Global Command and Control System-Joint	Maintained

JTF-GTMO Hosted and Maintained Software Applications

Joint Detainee Information Management System (JDIMS)	Maintained
Detainee Information Management System (DIMS)	Hoteled

JTF-Bravo Hoteled Systems

Name
Army Airfield Automation System (AAAS)
AAFES-PX
ACES-FD
AFAS
Armed Forces Health Longitudinal Technology Application (AHLTA)
Aviation Mission Planning System (AMPS)
APOSD
Army Food Management Info System (AFMIS)
ASR-11
Blue Force Tracker
BSM-E v2.0
CSEL
DEERS/Real-Time Automated Personnel Identification System (RAPIDS)
Defense Medical Logistics Standard Support (DMLSS)
Finance Defense MILPAY Office (DMO)
Joint Environment Toolkit (JET)
MEDWEB SVR
MCPP
MWR RECTRAC
NTFS/AFWA Weather
Property Book Unit Supply Enhanced (PBUSE)
RGATES Juniper VPN/Netscreen
Standard Army Ammunition System (SAAS)
Standard Army Maintenance System (SAMS)
Standard Army Retail Supply System (SARSS)
Standard Procurement System (SPS)
SPSI
Tactical Airspace Integration System (TAIS)
Tactical Meteorological Observing System (TMOS)
Unit Level Logistics System - Aviation (ULLS-A)

PART 7 – ATTACHMENT 11 – TECHNICAL EXHIBIT 11 – JIE Technical Implementation Guidelines

See Separate File

PART 7 – ATTACHMENT 12 - TECHNICAL EXHIBIT 12 - Reserved

PART 7 – ATTAHCMENT 13 - TECHNICAL EXHIBIT 13 – Functions Requiring Non-Disclosure Agreements

The Contractor personnel supporting the following functions require non-disclosure agreements.

Functions	Rationale
All personnel with elevated permissions to include any type of System Administrator or Network Administrator rights or personnel with remote access connections to a personal computer.	Contractor personnel have the ability to access need to know and privacy act information.
All personnel working at JTF-GTMO	Contractor personnel are supporting a mission with significant political sensitivities.

(b)(3):10 U.S.C. § 130,(b)(7)(E)

(b)(3):10 U.S.C. § 130,(b)(7)(E)

(b)(3):10 U.S.C. § 130,(b)(7)(E)

(b)(3):10 U.S.C. § 130,(b)(7)(E)

(b)(3):10 U.S.C. § 130,(b)(7)(E)

(b)(3):10 U.S.C. § 130,(b)(7)(E)

(b)(3):10 U.S.C. § 130,(b)(7)(E)

(b)(3):10 U.S.C. § 130,(b)(7)(E)

(b)(3):10 U.S.C. § 130,(b)(7)(E)

PART 7 – ATTACHMENT 18 - TECHNICAL EXHIBIT 18 – Life Cycle Related Projects

As of 11 Jan 2015

	Project
2	525TH - SharePoint Consolidation JIATF-S
3	525TH - 2003 Windows Server Upgrade
4	525TH - CISCO Identity Service Engine
5	525TH - CTOC Dashboard
6	525TH - EPM Rollout into J6
7	525TH - SCWFO VMware Implementation
8	525TH - SEI Exercise Support Event Time data Management
9	525TH - Service Now
10	525TH - SOUTHCOM COOP (DRSC) Phase III
11	525TH - SQL Server 2008 Upgrade
12	O 20131021 Office Upgrade
13	O 20131030 IdSS and FIM Proof of Concept
14	O A 20131029 Accountability Tracking and Data Call
15	O A 20131031 UAMS
16	O A 20131115 Accountability Tracking Tool Update
17	O A 20131119 508 Compliance
18	O A 20131220 SharePoint 2010 Post Migration
19	O E 20131029 Application Virtualization of Adobe Pro
20	O E 20131029 DoD Visitor on SIPR
21	O EN 20131029 TCSC 802 1x Implementation
22	O ES 20131029 AD DC Upgrade to Server 2008 R2
23	O ES 20131029 DMZ Server Separation
24	O ES 20131029 VMWare 5_1 and VCM Upgrade
25	O ES 20140724 DDS Network Funcionality Upgrade Implementation
26	O ESA 20140109 TAPES Tool LetterKenny CPAC
27	O H 20131029 AMHS Software Upgrade
28	O H 20131127 Mobile Device Software Upgrade
29	O N 20131029 CER E911 ALI Database Update
30	O N 20131029 RSA Two Factor Authentication
31	O N 20131029 UCCX Administrative Tool
32	O S 20131029 SIPR Printer Token
33	O S 20131029 SUP and SCUP Implementation
34	O-A_20130408_SharePoint2010_Migration_R2
35	ORS 20140528 FIM Implementation
36	OS 20131029 Mobility Classified Capability Pilot Program
37	R 20131029 Quarters One Renovation
38	R 20140422 Resource Activity Implementation
39	R 20140604 CCA VTC Upgrade
40	R I 20131029 Host Nation Rider Relocation
41	R L 20131031 MARFORSOUTH PC Monitor Lifecycle
42	RO 20140310 SPIAN IP Address Change
43	S C 20131029 Encase Forensic

PART 7 – ATTACHMENT 19 TECHNICAL EXHIBIT 19 – Level 1 and Level 2 Information Assurance Accreditation Package Work

Table 1 SIPRNET and NIPRNET Accreditation Packages

Approx. 50 Percent of the Packages are on SIPRNET and 50% on NIPRNET

Actual Data in Packages and Circuit Numbers by Network Are Classified and Will Be Provided during the Appropriate Phase-In Period

	SITE	TYPE	Level 2 IA - Review and Track	Level 1 IA - Maintain and Track
1	JIATF-S Special 1	[redacted]	X	
2	JIATF-S Special 2	[redacted]	X	
3	SOCSOUTH	[redacted]	X	
4	SOCSOUTH	[redacted]	X	
5	HQ SOUTHCOM	[redacted]	X	X
6	HQ SOUTHCOM	[redacted]	X	X
7	HQ SOUTHCOM	[redacted]	X	X
8	HQ SOUTHCOM	[redacted]	X	X
9	HQ SOUTHCOM	[redacted]	X	X
10	HQ Back-up	[redacted]	X	X
11	HQ Back-up	[redacted]	X	X
12	JIATF South	[redacted]	X	
13	JIATF South	[redacted]	X	
14	HQ SOUTHCOM	[redacted]	X	X
15	HQ SOUTHCOM	[redacted]	X	X
16	HQ SOUTHCOM	[redacted]	X	X
17	HQ SOUTHCOM	[redacted]	X	X
18	HQ SOUTHCOM	[redacted]	X	X
19	HQ Back-up	[redacted]	X	X
20	HQ Back-up	[redacted]	X	X
21	SCWFO ICAN U	[redacted]	X	X
22	SCWFO PSB	[redacted]	X	X
23	TCSC	[redacted]	X	X
24	TCSC	[redacted]	X	X
25	TCSC	[redacted]	X	X
26	TCSC	[redacted]	X	X
27	JIATF-S Special 3	[redacted]	X	
28	JTF-GTMO	[redacted]	X	X
29	JTF-GTMO	[redacted]	X	X
30	JTF-GTMO	[redacted]	X	X
31	JTF-Bravo	[redacted]	X	X
32	JTF-Bravo	[redacted]	X	X
33	JTF-Bravo	[redacted]	X	X
34	JTF-Bravo	[redacted]	X	X
	As of : 11-Jan-15			
		SIPRNet Circuit		
		NIPRNet Circuit		

Table 1 SIPRNET and NIPRNET Accreditation Packages Continued

Security Cooperation Office	NIPR	SIPR	Level 1 IA Develop Maintain	Level 2 IA - Review and Track
Argentina	X	X	x	x
Barbados	X	X	x	x
Belize	X	X	x	x
Bolivia	X	X	x	x
Brazil	X	X	x	x
Chile	X	X	x	x
Colombia - Bogota	X	X	x	x
Colombia - Cartagena	X	X	x	x
Columbia - Cartagena	X	X	x	x
Costa Rica	X	X	x	x
Curacao	X	X	x	x
Dominican Republic	X	X	x	x
Ecuador	X	X	x	x
El Salvador	X	X	x	x
Guatemala	X	X	x	x
Guyana	X	X	x	x
Haiti	X	X	x	x
Honduras	X	X	x	x
Jamaica	X	X	x	x
Nicaragua	X	X	x	x
Panama	X	X	x	x
Paraguay	X	X	x	x
Peru	X	X	x	x
Suriname (NIPR ONLY)	X	X	x	x
Trinidad & Tobago	X	X	x	x
Uruguay	X	X	x	x
Venezuela	X	X	x	x

Table 2 – Cross Domain Systems

A	B	C	D
Site	Cross Domain Solution Accreditionations	Level 1 IA	Level 2 IA
HQ SOUTHCOM	X	X	X
JIATF-S	X		X
JIATF-S	X		X
JIATF-S	X		X
JIATF-S	X		X
JIATF-S	X		X
Special Project	X		X

Table 3 – VTC Circuits

	B	C	D	E
	SITE ID	NETWORK	IA Level 1 - Maintain - Track	IA Level 2 - Review - Track
1	JIATF-S	SIPRNet		X
2	JTF-B	SIPRNet	X	X
3	JTF-B	SIPRNet	X	X
4	GTMO	DSN	X	X
5	GTMO	DSN	X	X
6	JTF-B	SIPRNet	X	X
7	JTF-B	SIPRNet	X	X
8	JTF-B	SIPRNet	X	X
9	JTF-B	DSN	X	X
10	JTF-B	DSN	X	X
11	JTF-B	SIPRNet	X	X
12	JIATF-S	NIPRNet		X
13	SOUTHCOM	NIPRNet	X	X
14	SOUTHCOM	NIPRNet	X	X
15	SOUTHCOM	NIPRNet	X	X
16	SOUTHCOM	NIPRNet	X	X
17	SOUTHCOM	NIPRNet	X	X
18	SOUTHCOM	NIPRNet	X	X
19	SOUTHCOM	SIPRNet	X	X
20	SOUTHCOM	SIPRNet	X	X
21	SOUTHCOM	SIPRNet	X	X
22	SOUTHCOM	SIPRNet	X	X
23	SOUTHCOM	SIPRNet	X	X
24	SOUTHCOM	SIPRNet	X	X
25	SOUTHCOM	SIPRNet	X	X
26	SOUTHCOM	SIPRNet	X	X
27	SOUTHCOM	SIPRNet	X	X
28	SOUTHCOM	SIPRNet	X	X
29	SOUTHCOM	SIPRNet	X	X
30	SOUTHCOM	SIPRNet	X	X
31	SOUTHCOM	SIPRNet	X	X
32	SOUTHCOM	SIPRNet	X	X
33	SOUTHCOM	SIPRNet	X	X
34	SOUTHCOM	SIPRNet	X	X
35	SOUTHCOM	SIPRNet	X	X
36	SOUTHCOM	SIPRNet	X	X
37	SOUTHCOM	SIPRNet	X	X
38	SOUTHCOM	SIPRNet	X	X
39	SOUTHCOM	SIPRNet	X	X
40	SOUTHCOM	SIPRNet	X	X
41	SOUTHCOM	SIPRNet	X	X
42	SOUTHCOM	SIPRNet	X	X
43	GTMO	DSN	X	X
44	GTMO	SIPRNet	X	X
45	GTMO	SIPRNet	X	X

Table 3 – VTC Circuits - Continued

45	GTMO	SPPNet	X	X
47	GTMO	SPPNet	X	X
48	GTMO	DSN	X	X
49	GTMO	SPPNet	X	X
50	GTMO	SPPNet	X	X
51	GTMO	SPPNet	X	X
52	GTMO	SPPNet	X	X
53	GTMO	SPPNet	X	X
54	GTMO	DSN	X	X
55	GTMO	SPPNet	X	X
56	GTMO	SPPNet	X	X
57	GTMO	SPPNet	X	X
58	GTMO	SPPNet	X	X
59	GTMO	DSN	X	X
60	GTMO	SPPNet	X	X
61	GTMO	SPPNet	X	X
62	GTMO	DSN	X	X
63	GTMO	SPPNet	X	X
64	GTMO	SPPNet	X	X
⋮		⋮		

Table 4– Hoteled or Hosted Special Hosted Systems -

	SYSTEM NAME	NETWORK	IA Level 1 - Maintain - Track	IA Level 2 - Review - Track
1	SOC System 1	SIPRNet		X
2	Internagency System 1	NIPRNet		X
3	Internagency System 2	NIPRNet		X
4	Voice over IP	SIPRNet	X	X
5	Directorate X	SIPRNet		X
6	Directorate X	Stand Alone		X
7	Army Project	NIPRNet	X	X
8	Army Project	SIPRNet	X	X
9	Army Project	SIPRNet	X	X
10	Special Proejct	SIPRNet		X
11	Classified Voice	SIPRNet	X	X
12	SATCOM	Stand Alone	X	X
13	Coalition System	SIPRNet	X	X
14	Equipment in the Pentagon	NIPRNet	X	X
15	Program of Record	NIPRNet	X	X
16	SOC Program of Record	SIPRNet		X
17	Program of Record	SIPRNet	X	X
18	Equipment in the Pentagon	SIPRNet	X	X
19	Special Location	SIPRNet	X	X
20	Special Location	SIPRNet	X	X
21	Special Location	SIPRNet	X	X
22	Special Location	SIPRNet	X	X
23	Special Location	SIPRNet	X	X
24	Special Location	SIPRNet	X	X
25	Training	15Mbps		X
26	Program of Record	NIPRNet	X	X
27	Program of Record	SIPRNet	X	X
28	Program of Record	SIPRNet	X	X
29	Program of Record	NIPRNet	X	X
30	Special Project	SIPRNet		X
31	Radios	Stand Alone	X	X
32	Directorate X	SIPRNet		X
33	Directorate X	NIPRNet		X
34	PDAs	SIPRNet		X
35	PDAs	NIPRNet		X
36	Army System X	NIPRNet		X
37	Army System X	SIPRNet		X
38	Army System X	NIPRNet		X
39	Navy System X	NIPRNet		X
40	SOUTHCOM System X	SIPRNet	X	X
41	Interagency System	NIPRNet		X
42	Interagency System	SIPRNet		X
43	Interagency System	SIPRNet		X
44	Interagency System	SIPRNet		X

Table 4– Hoteled or Hosted Special Hosted Systems - Continued

45	Interagency System	SIPRNet		X
46	Interagency System	Stand Alone		X
47	Interagency System	SIPRNet		X
48	Interagency System	NIPRNet		X
49	Program of Record	SIPRNet		X
50	Dod System X	NIPRNet		X
51	Dod System X	unknown		X
52	Dod System X	NIPRNet		X
53	Dod System X	NIPRNet		X
54	Dod System X	NIPRNet		X
55	Dod System X	unknown		X
56	Dod System X	NIPRNet		X
57	Dod System X	NIPRNet		X
58	Dod System X	NIPRNet		X
59	Dod System X	NIPRNet		X
60	Dod System X	NIPRNet		X
61	Dod System X	NIPRNet		X
62	Dod System X	NIPRNet		X
63	Dod System X	NIPRNet		X
64	Dod System X	NIPRNet		X
65	Dod System X	unknown		X
66	Dod System X	NIPRNet		X
67	Dod System X	NIPRNet		X
68	Dod System X	NIPRNet		X
69	Dod System X	unknown		X
70	Dod System X	unknown		X
71	Dod System X	NIPRNet		X
72	Dod System X	NIPRNet		X
73	Dod System X	NIPRNet		X
74	Intergency System	T1		X
75	Intergency System	T1		X
76	Intergency System	T1		X
77	Intergency System	T1		X
78	Intergency System	T1		X
79	Intergency System	T1		X
80	Intergency System	T1		X
81	Intergency System	T1		X
82	Intergency System			X
83	Intergency System	NIPRNet		X
84	Intergency System	NIPRNet		X
85	Intergency System	SIPRNet		X
86	Intergency System	SIPRNet		X
87	Intergency System	Stand Alone		X
88	Dod System X	SIPRNet		X

Table 4– Hoteled or Hosted Special Hosted Systems - Continued

89	Dod System X	SIPRNet		X
90	Dod System X	SIPRNet		X
91	Dod System X	SIPRNet		X
92	Dod System X	SIPRNet		X
93	Dod System X	SIPRNet		X
94	Dod System X			X
95	Dod System X			X
96	JIATF-S System			X
97	Program of Record	SIPRNet		X
98	Interagency System	SIPRNet		X
99	Lockheed System	Internet		X
100	Dod System X	Internet		X
101	Interagency System	Internet		X
102	Training	Internet		X
103	Training	Internet		X
104	Television	Internet		X
105	Dod System X	Internet		X
106	Multination Systems	A Network		X
107	Multination Systems	A Network		X
108	Multination Systems	A Network		X
109	Multination Systems	A Network		X
110	Multination Systems	A Network		X
111	Multination Systems	A Network		X
112	Multination Systems	A Network		X
113	Multination Systems	A Network		X
114	Multination Systems	A Network		X

PART 7 – ATTACHMENT 20 - TECHNICAL EXHIBIT 20 – Maintained Software Applications

1	Domain	Application	Application Type	Description	Future Migration Required
2	SIPR	Accountability Tracking	Web App	Schedule Accountability and HR datacalls	Possibly
3	NIPR	Accountability Tracking - Data Call	Web App	Used to execute and collect responses for accountability data calls	Possibly
4	SIPR	Address Verification System	Web, Library, Web Service	*Library, Service and Web management page to extend the Zip Code and address validation. Consumed by SCEMS*	Periodic
5	SIPR	Agreement (AUP)	Web App	Upon the first login, prompts user to accept the SOUTHCOM Acceptable Use Policy Agreement.	Yes
6	NIPR	AMA (Asset management Application; former "WASP")	Web App	Warehouse Asset Manager	Yes
7	SIPR	Athoc Integrator	Console	Used to integrate SCEMS with the ATHoc System	Periodic
8	NIPR	Awards	Web App (Site)	Process civilian honorary awards and military award actions.	Yes
9	SIPR	BlackBerry Tracker	Web App (Site)	*Black Berry Tracker web site to manage all Devices at HQ/Southcom*	Yes
10	SIPR	CBT Annual Security Awareness	Web Site (Flash)	SC required annual training.	Periodic
11	SIPR	CBT Command Security	Web Site (Flash)	*SC required annual training. Authorware CBT*	Periodic
12	NIPR	CBT Command Security	Web Site (Flash)	*SC required annual training. Authorware CBT*	Periodic
13	SIPR	CBT Counter Intelligence	Web Site (Flash)	SC required annual training.	Periodic
14	SIPR	CBT CyberAwarenessChallenge	Web Site (Flash)	SC required annual training.	Periodic
15	NIPR	CBT CyberAwarenessChallenge	Web Site (Flash)	SC required annual training.	Periodic
16	NIPR	CBT Hurricane Prep 2013	Web Site (Flash)	SC required annual training.	Periodic
17	SIPR	CBT Hurricane Prep 2013	Web Site (Flash)	SC required annual training.	Periodic
18	NIPR	CBT Information Assurance Awareness	Web Site (Flash)	**DB Notes indicate that this application is deprecated.** CBT Training	Periodic
19	SIPR	CBT Intelligence Oversight (SIPR)	Web Site (Flash)	*SC required annual training. Production URL : http://scems/cbtcourses/inteloversight/inteloversight7.htm*	Periodic
20	SIPR	CBT Level 5 Refresher	Web Site (Flash)	SC required annual training.	Periodic
21	SIPR	CBT OPSEC Annual Refresher	Web Site	*SC required annual training.*	Periodic
22	SIPR	CBT OPSEC INITIAL SIPR	Web Site	*SC required training, taken upon onboarding.*	Periodic
23	NIPR	CBT Southern Exposure Volume 1,2,3,4,5,7	Web Site (Flash)	*SC required annual training. Flash Game/Quiz*	Periodic
24	SIPR	CBT Training Due	Web Part	*CBT Training Due SIPR sharepoint webpart. Displays the current status of an individuals SC required training.*	Yes
25	NIPR	CBT Training Due	Web Part	*CBT Training Due SIPR sharepoint webpart. Displays the current status of an individuals SC required training.*	Yes
26	SIPR	Contingency Operations	Web App (Site)	System to setup for Manning and monitor readiness for Contingencies	Periodic
27	SIPR	Data File Replication System	Web, Library, Windows	*System to setup and execute data and file transfer in disconnected states. Management web, business and data libraries, and windows application for client routines execution.*	Yes
28	NIPR	Extranet Users Site	Web App (Site)	*Website code for external people to logon sipr. First you must give information(name, rank, service, directorate, email) for approval.*	Yes
29	NIPR	ExtranetUserMaintenance	Win App	*Maintains external user logins. Sends emails to users and sponsors when login expiration is close or to change password. Deletes old logins.*	Yes
30	NIPR	Folder Move Tool	Web App	Used during the Consolidate JCode cleanup project	Possibly
31	SIPR	Folder Move Tool	Web App	Used during the Consolidated JCode cleaneup project	Possibly
32	SIPR	ILM	Library	*Information Lifecycle Management SQL View*	Possibly
33	NIPR	LEAPS V2	Web App	Connects user accounts to CAC Cards.	Possibly
34	NIPR	New Arrival Tracker System	Web App	Information repository and automated workflow designed to facilitate and audit the distribution of relocation information to newly processed SOUTHCOM personnel and their spouses.	Yes

Maintained Software Applications - Continued

40	SIPR	SCEMS HRIS/Mission Management	Web App (Site)	Used to Setup and manage missions and mission personnel and augmentee information	Yes
41	SIPR	SCEMS HRIS/My Info	Web App (Site)	Used to access personal info in scems	Yes
42	SIPR	SCEMS HRIS/Process Change Requests	Web App (Site)	Manages the workflow for requests for change to personnel data	Yes
43	SIPR	SCEMS INFO/ContactLists	Web App (Site)	Used by Help Desk to view User information	Yes
44	SIPR	SCEMS INFO/Information	Web App (Site)	Used to access SCEMS information on the SC Intranet	Yes
45	SIPR	SCEMS Job Scheduler	Console	*Runs SCEMS scheduled tasks*	Yes
46	SIPR	SCEMS On-Boarding HRIS /InProcess Directorate	Web App (Site)	Part of SCEMS on-boarding workflow	Yes
47	SIPR	SCEMS On-Boarding HRIS /Awaiting Processing	Web App (Site)	Part of SCEMS on-boarding workflow	Yes
48	SIPR	SCEMS On-Boarding HRIS /Process Assigned	Web App (Site)	Part of SCEMS on-boarding workflow	Yes
49	SIPR	SCEMS SECURITY /AccountDisable	Web App (Site)	Used to Disable user's network accounts	Yes
50	SIPR	SCEMS SECURITY /BarredAccess	Web App (Site)	Used to Bar user's access to networks	Yes
51	SIPR	SCEMS SECURITY /InProcessSecurity	Web App (Site)	Part of SCEMS on-boarding workflow	Yes
52	SIPR	SCEMS SECURITY/SecurityAdmin	Web App (Site)	Used by Security to Administer security related issues for SC personnel	Yes
53	SIPR	SCEMS SECURITY/UsersSecurity	Web App (Site)	Used to display clearance information for SC personnel.	Yes
54	SIPR	SCEMS SUPPORT/Application Administration	Web App (Site)	Used to Assign Permission Levelsin SCEMS	Yes
55	SIPR	SCEMS SUPPORT/DataCall Manager	Web App (Site)	Used to schedule and track responses for HR and Accouintability datacalls	Possibly
56	SIPR	SCEMS SUPPORT/Developer Admin	Web App (Site)	Used by AppDev to manage SCEMS pages	Possibly
57	SIPR	SCEMS SUPPORT/Help	Web App (Site)		Possibly
58	SIPR	SCEMS SUPPORT/Network Service Wizard	Web App (Site)	Used to process network related requests	Yes
59	SIPR	SCEMS SUPPORT/Office Codes	Web App (Site)	Used to Manage office code hierarchy and group level personnel assignments	Yes
60	SIPR	SCEMS SUPPORT/Reports	Web App (Site)	Reporting Services for SCEMS data	Possibly
61	SIPR	SCOMSqlHelper	Web App	Used to monitor production server performance	Possibly
62	NIPR	SCOMSqlHelper	Web App	Used to monitor production server performance	Possibly
63	SIPR	SCPortal	Web Portal	SIPR Enterprise Sharepoint Portal	Life Cycle Upgrades based on SharePoint Life Cycle
64	NIPR	SCPortal	Web Portal	NIPR Enterprise Sharepoint Portal	Life Cycle Upgrades based on SharePoint Life Cycle
65	SIPR	Sharepoint File Search	Win App	*Utility to search sharepoint for files and batch download results to a file location or sharepoint library*	Life Cycle Upgrades based on SharePoint Life Cycle
66	NIPR	SharePoint People Search	Web Site	Enterprise search center	Life Cycle Upgrades based on SharePoint Life Cycle
67	NIPR	Southcom.mil	Web Portal	Public SC Site	Life Cycle Upgrades based on SharePoint Life Cycle
68	SIPR	SPFocalPoint	Web App (Site)	*Allows external users to change security questions. Allows sponsor to give user permissions. Allows accounts for those who need to post to SOUTHCOM SharePoint Portal or for access to specific limited-access sites. Can import users to system. Allows users to retrieve passwords or change passwords. Generates list of WIC Users Approval Status to be printed or inserted into excel. This is ready to write to active directory.*	Life Cycle Upgrades based on SharePoint Life Cycle
69	NIPR	Sustainment Training	Web Site	Adminstration of classes, cots, attendance, and scoring. *Training HTTP handler wrapper modules. Training class registration module.*	Yes
70	SIPR	Sustainment Training	Web Site	Adminstration of classes, cots, attendance, and scoring.	Yes
71	SIPR	SysTrays Announcements	Win App	*Systray Announcement Client, Designer, Code Manager, Rules for SIPR*	Yes
72	NIPR	SysTrays Announcements	Win App	*Systray Announcement Client, Designer, Code Manager, Rules for NIPR*	Yes
73	NIPR	Vendor Submissions	Web App (Site)	*Vendors Submissions Website for the low sides. Out of use. Used to track vendor information.*	Yes
74	SIPR	Web Tabs	Web, Console, ActiveX	*Web application with SCEMS, client console app, and ActiveX component. System to track and maintain client sites. Consider Deprecation.*	Yes

Current Application Development Projects

Priority	Name	Description / Objective
Projects		
	User Account Management System (UAMS) couple with IDSS	To consolidate the Command's various user account registration processes into a single scalable registration and account maintenance system
	(CBT) Framework	Create a framework for creating CBTs that can be used by non-developers.
	SCEMS - Move SCEMS to NIPR	Initially to provide in-process functionality to the Garrison and Clinic. Will also accommodate eternal data calls
	SCEMS - Electronic Org Chart	New functionality in SCEMS
	SCEMS - Evaluation Tracker	New functionality in SCEMS
	Enterprise Gateway Services (EGS)	
	Service Now Implementation	
	Reporting server upgrade	
O & M		
	Contingency Operations	Update / Modifications / Bug Fixes
	New Arrival Tracking	Update / Modifications / Bug Fixes
	BlackBerry Tracker Updates	Update / Modifications / Bug Fixes
	Data File Replication System	Update / Modifications / Bug Fixes
	Data Call/ Accountability Tracker	Update / Modifications / Bug Fixes
	Awards Manager	Update / Modifications / Bug Fixes
	CBTs	Update / Modifications / Bug Fixes
	Sharepoint Requests	Administration / Custom Development
	SCEMS	Operational Support/Bug Fixes
	Extranet User Accounts maintenance/support	Operational Support/Bug Fixes
Other Initiatives		
	Regression Testing	Create / Maintain regression test suites Automate test suites

PART 7 – ATTACHMENT 21 - TECHNICAL EXHIBIT 21 – Organizational Background Information

Basic information on HQ SOUTHCOM can be found on the following homepage.

http://www.southcom.mil/aboutus/Pages/About-Us.aspx

Information on other organizations supported by this effort can be found here:

http://www.southcom.mil/aboutus/Pages/Our-Team.aspx

Equipment Count and Ageing Information

All Requirements Combined					Age in Years			
Items	SIPRNET	NIPRNET	Other		0 to 2	3 to 4	5 to 6	7 or more
Number of PCs	3634	5716	0		x	x	x	
Number of Physical Servers	77	127	0		x	x	x	
Number of Virtual Servers	316	439	0		x	x	x	x
Number of Physical Servers (Voice)	6	59	14		x		x	
Number of Virtual Servers (Voice)	0	70	0			x		
Number Routers	14	71	28				x	
Number of Type 1 Encryption Devices	670	200	10		x	x	x	x
Number of Telephone Switches	56	57	2		x	x	x	
Number of Network Switches	350	518	22		x		x	
Number of Terminal Servers	118	119	2				x	
Number of Firewalls	34	36	4		x	x		
Number of IPS/IDS	10	10	1			x		
Number of Other Info Assurance Devices	22	28	0			x		
Number of Conferences Rooms with VTC	87	67	0		x	x	x	x
Permanent Training Rooms - Capacity	0	1	0					
Number of Secure Phone Instruments (STE/VIPERs)	1160	300	17		x	x	x	x
Number of VOIP Phones	4	1500	0				x	
Number of Plain old Telephone	0	255	2500		x		x	
Data Center Infrastructure (Racks Power, Cooling, UPS, Fire Suppression, Matrix Switches etc.)	0	0	1				x	x
Number of Multi-Function Printer/Scanners	106	343	0		x	x	x	
Total								

TCSC Data					Age in Years			
	SIPRNET	NIPRNET	Other		0 to 2	3 to 4	5 to 6	7 or more
Number of PCs	252	817			x	x		
Number of Physical Servers	11	55			x		x	
Number of Virtual Servers	58	175						
Number of Physical Servers (Voice)	6	53	14		x		x	
Number of Virtual Servers (Voice)		58				x		
Number Routers								
Number of Type 1 Encryption Devices	160	200	10		x	x		
Number of Telephone Switches	56	56	1				x	
Number of Network Switches	10	10	2		x			
Number of Terminal Servers	6	7					x	
Number of Firewalls								
Number of IPS/IDS								
Number of Other Info Assurance Devices	10	12				x		
Number of Conferences Rooms with VTC	27	6			x	x		x
Permanent Training Rooms - Capacity								
Number of Secure Phone Instruments (STE/VIPERs)								
Number of VOIP Phones								
Number of Plain old Telephone								
Data Center Infrastructure								
Number of Multi-Function Printer/Scanners	30	64			x	x	x	

JTF-GTMO Data					Age in Years			
	SIPRENT	NIPRNET	Other		0 to 2	3 to 4	5 to 6	7 or more
Number of PCs	669	1188					x	
Number of Physical Servers	27	27				x		
Number of Virtual Servers	101	70				x		
Number of Physical Servers (Voice)								
Number of Virtual Servers (Voice)								
Number Routers	6	34	14				x	
Number of Type 1 Encryption Devices	67							x
Number of Telephone Switches	0	0				x		
Number of Network Switches	160	200	10				x	
Number of Terminal Servers	56	56	1				x	
Number of Firewalls	16	17	2		x			
Number of IPS/IDS								
Number of Other Info Assurance Devices	2	3				x		
Number of Conferences Rooms with VTC	9	9						
Permanent Training Rooms - Capacity		1						
Number of Secure Phone Instruments (STE/VIPERs)			17					x
Number of VOIP Phones	0	0	0					

Number of Plain old Telephone							x	
Data Center Infrastructure								
Number of Multi-Function Printer/Scanners	5	41				x		

JTF-Bravo Data					Age in Years			
	SIPRENT	NIPRNET	Other		0 to 2	3 to 4	5 to 6	7 or more
Number of PCs	108	876				x		
Number of Physical Servers	5	7					x	
Number of Virtual Servers	9	17					x	
Number of Physical Servers (Voice)								
Number of Virtual Servers (Voice)								
Number Routers	2	3					x	
Number of Type 1 Encryption Devices	14	0				x		
Number of Telephone Switches			1		x			
Number of Network Switches	20	108					x	
Number of Terminal Servers	0	0					x	
Number of Firewalls	2	2				x		
Number of IPS/IDS	2	2				x		
Number of Other Info Assurance Devices	8	10				x		
Number of Conferences Rooms with VTC	5	6					x	
Permanent Training Rooms - Capacity	0	0						
Number of Secure Phone Instruments (STE/VIPERs)	40	0				x	x	
Number of VOIP Phones	0	0					x	
Number of Plain old Telephone					x			
Data Center Infrastructure								
Number of Multi-Function Printer/Scanners	11	146				x		

525th Data					Age in Years			
	SIPRENT	NIPRNET	Other		0 to 2	3 to 4	5 to 6	7 or more
Number of PCs	2605	2835			x	x	x	
Number of Physical Servers	34	38			x	x	x	
Number of Virtual Servers	148	177			x	x	x	x
Number of Physical Servers (Voice)		6						
Number of Virtual Servers (Voice)		12						
Number Routers	6	34	14				x	
Number of Type 1 Encryption Devices	429				x	x	x	
Number of Telephone Switches		1				x		
Number of Network Switches	160	200	10				x	
Number of Terminal Servers	56	56	1				x	
Number of Firewalls	16	17	2		x			
Number of IPS/IDS	8	8	1			x		
Number of Other Info Assurance Devices	2	3				x		
Number of Conferences Rooms with VTC	46	46						
Permanent Training Rooms - Capacity								
Number of Secure Phone Instruments (STE/VIPERs)	1120	300			x	x	x	x
Number of VOIP Phones	4	1500					x	
Number of Plain old Telephone		255					x	
Data Center Infrastructure								
Number of Multi-Function Printer/Scanners	60	92						

JTF-GTMO
Historical Data

- ***JTF Mission Statement***
  - Core Missions
    - Safe, Humane, Legal and Transparent Care and Custody of Detainees
    - Intelligence collection, analysis and dissemination
    - Support of Office of Military Commissions
  - Collateral Support
    - Mass migration
    - Cuban instability

- ***JTF J6 Mission Statement***
  - "Provide secure integrated, responsive, reliable, communications and information systems supporting Joint Task Force detention for the safe, humane, legal and transparent care and custody of detainees, detainee ops, intelligence ops, migrant ops & commission trials."

- ***JTF J6 AOR/Functional Structure***
  - Future Ops Division
    - Program Management, Engineering, Installs, Requirements, Site Surveys, Contract Management
  - Current Ops Division
    - Network Management, System Administration, Telephones, Radios, Help Desk, VTC, GCCS, JWICS
  - Information Assurance Division
    - C&A, COMSEC, Info Assurance, Firewall, Bluecoat HBSS, CND, Policy
  - Plans & Resources Division
    - Plans, Programs, Budget, Acquisition, GPC, Configuration Management, Asset Management

- ***Footprint***
  - NIPR (Non-classified Internet Protocol Router)
    - 2100 user accounts
    - 1186 computers
    - 101 servers
    - 1 core site, 7 distribution sites, 98 access sites
  - SIPR (Secret Internet Protocol Router)
    - 1500 user accounts
    - 720 computers
    - 89 servers

        - 1 core site, 7 distribution sites, 67 access sites
    - JWICS (Joint Worldwide Intelligence Communication System)
        - 200 user accounts
        - 130 computers
        - 1 core site, 2 access sites
    - LMR (Land Mobile Radio)
        - Motorola Trunking System
        - 730 devices
    - JDIMS (Joint Detainee Intelligence Management System)
        - Web Based App – SIPR/JWICS
        - Contains local and off-island users

- ***Annual Metrics*** *(This information is not exact / mission demands dictate level of support)*
    - Help Desk Trouble Tickets – 3600 / 7000 walk-ins
    - NOC – 95% virtualized
    - Telecomm Trouble Tickets – 110 / 500 walk-ins
    - ITRs – 740
    - Projects – 60; small and large
    - Cell Phones – 580 users
    - LMRs – Motorola Trunking; 730 devices
    - VTC – 18 sys / 250 events
    - Accreditation Packages – 20
        - *NIPR, SIPR, JIOC-S, LMR, ISDN VTC, IP VTC*
        - *Standalone Specialty Systems*
    - Inspections – two a year DISA/SOUTHCOM IG

- ***NAVSTA / OMC***
    - NAVSTA– Naval Station Guantanamo
        - BCO (Base Communications Office)
            - Network
            - Telephone
        - ISD (Information System Department)
            - Cell Phone
            - LMR
        - NAVSTA Hospital
    - OMC (Office of Military Commissions)

JTF-Bravo Historical Data

JTF-B Mission Statement

- Core Missions
    - Counter-Transnational Organized Crime
    - Humanitarian Assistance/Disaster Relief
    - Building Partnership Capacity
- Collateral Support
    - Contingency Exercises
    - Regional collaboration and synchronization

JTF-B Mission Statement

Joint Task Force Bravo, as guests of our Honduran host nation partners and the senior representative for USSOUTHCOM at Soto Cano Air Base, conducts and supports joint operations, actions, and activities throughout the joint operations area maintaining a forward presence in order to enhance regional security, stability, and cooperation."

JTF J6 AOR/Functional Structure

- Network Operations (NETOPS) Division
    - Telephone Switch, Inside Plant, Outside Cable Plant, Telecommunications Services, Main Distribution Frames, Power Distribution, Rectifiers, Battery Banks, UPS, Generators, Air Conditioners, Giant Voice (PA) Systems, Microwave Systems, Special circuits, Long-haul circuits, Operator services,

    - Network Management/Administration, Systems Administration, Infrastructure, Help Desk, VTC, Land Mobile Radio Network; Frequency Management, Tactical systems

    - ADPE Engineering, Webmaster, Infrastructure Engineering, Draftsman

- Information Assurance Division
    - DIACAP C&A, COMSEC, Info Assurance, IAVAs, Firewall, HBSS, CND, Policy, PKI, Tokens, Inspections

- Proxy Servers, VPN Concentrators, Top Level Architecture

- Plans , Programs & Policy
    - Plans, Programs, Budget, Acquisition/Procurement, Configuration Management, Asset Management, Logistics, Transportation,

Draftsman, Official mail (Past averages: Incoming mail - 250 pieces/month, Outgoing mail – 100 pcs/mo, Stamps –Approx $500/mo)

Program/Project Management, Systems Engineering, Installs, Requirements, Site Surveys, Contract Management

Footprint (Numbers and metrics based on information collected over the past year)

- NIPR (Non-classified Internet Protocol Router) • 1200+ user accounts
- 881 computers
- 30 servers
- 1 core site, 1 distribution site, 81 access sites

- SIPR (Secret Internet Protocol Router) • 250 user accounts
- 133 computers
- 30 servers
- 1 core site, no distribution sites, 7 access sites

- LMR (Land Mobile Radio) • Motorola Radio System
- 243 devices

• ***Annual Metrics*** *(This information is not exact / mission demands dictated level of support)*
• Help Desk Trouble Tickets – 3,744

- NOC – 95% virtualized
- Telecomm Trouble Tickets – 1,104
- ITRs – 191
- Projects – 8 small and 10 large
- Blackberry licenses - 120
- Cell Phones – 200+ (Contract is handled/managed by the JTF-B J6 staff)
- LMRs – Motorola Trunking;
- Radios - 243
- VTC – 14 sys (Class/Unclas) / 50 VTCs per month avg.
- Accreditation Packages - 6 • *NIPR, SIPR, LMR, VTC (Class/Unclas), TELEPHONE*
- *Standalone Specialty Systems (PM Systems) – 27 (No MOU/MOAs with system owners)*

- Inspections – DISA IARR/SOUTHCOM IG/SOUTHCOM IA SAV/COMSEC

• Major Tenant Organizations

- JTF-B (Joint Task Force-Bravo)
- ASA/IMCOM (Army Support Activity/Installation Management Command)
- JSF (Joint Security Forces)
- ARFOR (Army Forces Battalion)
- 1/228th Aviation Regiment
- 612th Air Wing
- MEDEL (Medical Element)

TCSC Historical Data

TCSC AOR/Functional Structure

- Program Management
  - Program Manager, Deputy Program Manager, Program Administrative Staff
- Enterprise Operations
  - Systems Administration, Network Administration, On Site Technical Representatives (OSTRs), Engineering, Patch Management, VSAT Management
- Cyber Security
  - HBSS/CND Management, Accreditation/Compliance/Policy Management, COMSEC
- Logistics
  - Warehouse Management, Procurement, Configuration Management (CM), Pouching/Shipping

Footprint

- 27 Countries w/39 total Sites Supported across the AOR
- 59 DTS-PO Circuits
- 9 DISA Circuits
- 5538 Trouble Tickets Processed in 2014
- NIPRnet (Non-Classified Internet Protocol Routed network)
  - 1000 User Accounts
  - 841 Workstations
  - 25 Physical Servers
  - 24 SANs
  - 150 Virtual Servers
  - 2 Forefront TMGs (Threat Management Gateways (Reverse Proxy))
  - 102 MFPs
  - 3 Plotters
  - 20 Dell DR4100 Backup Appliances
  - 58 Routers
  - 4 Firewalls
  - 9 IP/IDS'
  - 12 VSAT Modems
  - 1 VSAT Hub
  - 100 Switches
  - 4 Riverbed SteelHead
  - 35 TACLANE Inline Network Encryptors (INEs) (KG-175D)
  - 8 VTC (TelePresence)
- SIPRnet (Secret Internet Protocol Routed network)
  - 380 User Accounts
  - 350 Workstations (295 TEMPEST & 55 Non-TEMPEST)
  - 15 Physical Servers
  - 4 SANs
  - 35 Virtual Servers

- 54 MFPs (52 TEMPEST & 2 Non-TEMPEST)
- 6 Plotters
- 40 Switches
- 5 Riverbed SteelHead
- 26 Secure VTCs (TEMPEST)

Additional Information

- All Servers are virtualized
- 405 Blackberry Users
- 56 Accreditation Packages
- 45 Expansion Projects across the AOR
- 60% of NIPR Users migrated to DEE (Migrated is defined as the user has stopped using TCSC email/exchange completely)
    - Users in Bogota, Colombia (50% of TCSC user base) have not fully migrated due to the "Foreign National" situation and not being able to share calendars with these users until they are migrated to DEE.
- 51 Organizational Mailboxes (OMBs) still residing in the TCSC Exchange environment
    - As we migrate to DEE we are trying to migrate these OMBs to Mail Enabled Security Groups (Distro Lists)
- 91 DEE Mail Enabled Security Lists managed by TCSC

PART 7 - Attachment 22 - Technical Exhibit 22 – JTF-Bravo Unique Services

1. The Contractor shall provide on-site support to JTF-B's Joint Operations Center (JOC) from 07:00 to 19:00 CST.

2. Miscellaneous Government Provided Services: The Government will provide customs exemptions and coverage or protection under the appropriate agreements with the Government of Honduras. American Red Cross services, such as emergency family communications and guidance for bereavement airfare are also available to United States citizen Contractor personnel overseas. The Government will make available to Contractor personnel, all documents and information the Government deems necessary for the Contractor to perform under this Task Order

3. Contractor personnel, whether CAAF (Contractors Authorized to Accompany the Force) or Non-CAAF, are authorized access to and use of certain US Government facilities at Soto Cano Air Base, Honduras. Authorized facilities include: Military/Base Exchange; military postal system; Morale, Welfare, and Recreation (MWR) facilities; and dining facilities. All items bought in the US Military Exchange shall be for personal use or consumption only and shall not be sold or used for commercial purposes. The Government reserves the right to withhold the privileges from any contract personnel in case of abuse. Access to MWR facilities and services do not extend to MWR facilities, trips, or activities outside Soto Cano Air Base, Honduras.

4. If required, the Contractor shall retain medical and dental insurance coverage on the local economy for personnel working at JTF-Bravo.

5. CAAF personnel are authorized use of military banks and/or credit unions (finance services only) as well as base fueling stations.

6. Reserved

7. Contractor personnel may only receive medical care from the JFT-B Medical Element (MEDEL) to prevent loss of life, limb or eyesight.

8. Other services may be available for either CAAF or Non-CAAF personnel dependent upon base/mission/operations support requirements and availability.

9. Utilities: All utilities at the Soto Cano Air Base will be available for the contractor's use in performance of tasks outlined in this PWS. The Contractor shall instruct personnel in utilities conservation practices. The contractor shall be responsible for operating under conditions that preclude the waste of utilities.

10. Use of Government Vehicles: The Government shall provide vehicles for use on this Task Order. Contractors will be permitted to use Government Furnished Vehicles pursuant to their

duties in this PWS, IAW JTF-B's policies. Examples may include access to specifically restricted areas for which pre-specified Contractor personnel require access.

11. The Contractor shall maintain all demarcation locations that support telephone, LAN (SIPRNET and NIPRNET), video teleconferencing (SIPRNET and NIPRNET), and data circuits in Soto Cano Air Base. The Contractor shall maintain and expand the U.S. military cable plant for Soto Cano Air Base; this includes all cable and wire installed for all Information Mission Area (IMA) requirements for telephones, special circuits, LAN, data circuits and video. The Contractor shall provide maintenance service, repair, training, and frequency management, for all tactical and non-tactical radios, satellite systems, and wireless LAN/WAN systems, to include all associated components of hardware and software. Systems include SECRET (S), SENSITIVE BUT UNCLASSIFIED (SBU), and UNCLASSIFIED (UNCLAS).

12. Remedy Enterprise BMC ITSM. The Contractor shall use the Remedy system to maintain the trouble ticketing tracking processes, provide administration of new and existing user accounts, provide training, training documentation, generate reports, maintain user data, quality control, and monitoring of all Soto Cano Air Base C4 Systems, workstations, printers, servers, infrastructure, software, warranties, and inventory data. As part of the consolidation of the Service Desk function at SC HQ, the Contractor shall transition to use of a single SOUTHCOM trouble ticketing system.

13. Remote Location Support. For remote locations, during normal working hours, the contractor shall dispatch personnel within 90 minutes from notification of an outage or serious impairment to transmission, switching, and command and control system failures on the most direct and safest manner. For the purposes of this PWS, remote locations are defined as Cerro El Horno, Cerro La Mole, and U.S. MILGRP at Tegucigalpa, Honduras. The ACOR can grant waivers on a case-by-case basis for maintenance response times. The Contractor shall receive, document, assign, monitor, and close Service Requests from customers. The Contractor shall open service request within 30 minutes of notification.

14. Base Communications Systems and Services Support. The Contractor shall operate and maintain (O&M) the telephone switching systems, premises equipment, ancillary equipment, cable infrastructure, and internal/external networks necessary to deliver electronic information to all customers in Soto Cano Air Base and SCO, Tegucigalpa.

14.1 Telephone Services – Main Switching Unit (MSU). Local Foreign Nationals are authorized for telephone systems requirements. The Contractor shall administer, operate and maintain a Government furnished (GFE) common user telephone Main Switching Unit (MSU), with full DISN capabilities and interoperability, and perform upgrades and modifications as required.

14.1.1 The Contractor shall install, configure, program, test, and maintain the additional equipment necessary to increase the MSU-equipped and wired line capacity as needed to support mission requirements. The existing Nortel SL-100 shall be replaced by an AVAYA Aura

CM6 VoIP enabled Small Medium Enterprise Office (SMEO) system, a CAIRS.Net Unique Telephony Management System (TMS), and a Sonexis Conference Manager. The AVAYA CM6 is licensed for 2184 analog and 208 digital stations. The Sonexis Conference Manager can support up to 96 ports for pre-set conference bridges. These bridges support Public Address (PA)/Giant Voice system, Joint Security Forces (JSF) Watch Towers, Secondary Crash Conference, Emergency 911, and "meet-me" conferences.

14.1.2 Remote Switching Units (RSUs). The Contractor shall operate and maintain (O&M) all common user telephone RSUs installed in Soto Cano Air Base and the MILGRP in Tegucigalpa, and perform upgrades and modifications as required. The Contractor shall install, configure, program, test, and maintain the additional equipment necessary to increase the RSU-equipped and wired line capacity as needed to support mission requirements. The new AVAYA RSU in R-29 is equipped with 696 analog and 72 digital lines. The new AVAYA RSU in S-73 is equipped with 168 analog and 24 digital lines. The new AVAYA RSU in MILGRP Tegucigalpa is equipped with 96 analog and 0 digital lines. The Contractor shall install, test and maintain the required additional connectivity from the RSUs to the MSU in order to ensure the RSUs traffic service requirements are met.

14.1.3 Telephone Firewall. The Contractor shall be required, at the request of the Government, to O&M an installation telephone switch firewall.

14.1.4 Operator Services. The Contractor shall provide common user automated attendant services. The Contractor shall provide temporary operator services during outages that affect the automated attendant system, emergencies, or contingencies as required by the Government.

14.1.5 Voice Mail Services. The Contractor shall operate and maintain the existing voice mail system. Contractor shall program/modify/delete users as required. Voice Mail shall be activated only for offices, with some exceptions approved by the JTF-B J6, designated Government representative, or the COR.

14.1.6 The Contractor shall operate and maintain the existing interfaces with the Cairs.NET Telephony Management System (TMS).

14.1.7 The Contractor shall maintain, program, and update Personal Identification Numbers (PIN) for assigned personnel as required or requested by JTF-B J6. This function is required to control commercial calls to the PSTN. The Contractor shall review usage reports, monitor for potential fraud, and notify JTF-B J6 or designated Government representative of the findings.

14.1.8 The Contractor shall maintain the current PBX services provided to the Honduras Air Force (HAF). The Contractor shall provide telephone access to multiple Honduran officials located on Soto Cano Air Base. Currently, there are approximately 90 telephone lines servicing

Honduran officials and guards. Upon JTF-B J6 or COR approval, the contractor shall install/de-install and maintain additional GFE phone services for the Honduran Air Force.

14.2 Installation Infrastructure

14.2.1 The Contractor shall provide Promina node site management and maintenance services for mission-specific requirements.

14.2.2 The Contractor shall inspect and maintain underground cable enclosures (manholes, hand-holes, pull-holes, and vaults). The Contractor shall address work in an attachment to the Service Operations and Maintenance Plan (Deliverable 22, Attachment 1).

14.2.1 The Contractor shall maintain an electronic & hard copy Plant in Place (PIP) drawing library. Redline drawings shall be completed within three days of required changes.

14.2.2 The Contractor shall operate and maintain common core (backbone infrastructure) voice/telephony network infrastructure equipment.

14.2.3 The Contractor shall provide access to third party telecom equipment maintenance personnel, whether Government or contracted.

14.2.4 The Contractor shall assist during Installation Information Infrastructure modernization efforts, Military Construction Army (MCA) projects; major or minor, Sustainment, Restoration, Modernization (SRM), and local construction/renovation/expansion projects at Soto Cano Air Base.

14.2.5 The Contractor shall assist the Government during the design, engineering, installation, configuration, maintenance, and repair of Wireless Network Access Points to support access to the installation infrastructure.

14.2.6 The Contractor shall administer, operate, and maintain the existing interoperability between the telephone and public address (PA) system.

14.2.7 The Contractor shall design, install/de-install, and maintain a Protective Distribution Systems (PDS).

14.2.8 Special Circuits; Fire, Safety, Security. The Contractor shall design, install/de-install, and maintain required circuits for fire, intrusion alarms, and other safety/security systems.

14.3 Outside Cable Plant (OCP) Cable Summary. Soto Cano Air Base cabling is comprised of copper (metallic) and fiber optic cabling, both Single Mode (SM) and Multi-Mode (MM). Both copper and fiber can run aerial (overhead) or underground (direct buried or ducting system).

14.3.1 The Contractor shall install/de-install, maintain, and repair all cable supporting special circuits; safety, security, fire alarms, intrusion alarms, emergency intercoms, telemetry, and other monitoring and control systems. This also includes all cable in Government quarters. Aerial runs, utility poles will be provided GFE. Procurement of material and parts shall be approved by the Government and provided as GFE.

14.4. Inside Cable Plant (ICP) for New Construction. The Contractor shall design, install/de-install, test and maintain the inside cable plant required to extend the Soto Cano Air Base LAN and telephone systems to new facilities constructed in Soto Cano Air Base during the Task Order period of performance. Procurement of material and parts shall be approved by the Government and provided as GFE.

14.5 Inside Cable Plant (ICP) and Outside Cable Plant (OCP). Local Foreign National personnel are authorized to support Unclassified ICP and OCP. The Contractor shall maintain the existing U.S. military inside and outside cable plant for the Soto Cano Air Base LAN, telephone systems, and data circuits. The cable and fiber optics plant carry connectivity for information systems, alarms, sensors, and intrusion detection systems as pertain to the network. At a minimum, the Contractor ensure two support personnel supporting these functions have Secret security clearances.

14.5.1 The Contractor shall install/de-install GFE conduit when required. The Contractor shall create, update, and maintain diagrams and records of existing and future LAN, fiber, and telephone communication lines as configuration changes are made to the Soto Cano Air Base IT infrastructure. The Contractor shall complete the appropriate form (digging permit) and submit it to Base Civil Engineering (BCE) for approval any time the Contractor needs to break ground.

14.5.2 The Contractor shall provide qualified, licensed drivers for the operational use of any specialty vehicle required by the contractor in the performance of this Task Order. The drivers can be local Foreign National personnel.

14.6 Main and Line Distribution Frames. The Contractor shall provide operations and maintenance support for the existing Main Distribution Frame (MDF) installed in Building A-47; the existing Line Distribution Frames (LDF) installed in Building R-29, S-73 Remote Switching Units (RSU) at Soto Cano Air Base, and the Wiring Distribution System located in the US MILGRP RSU in Tegucigalpa, Honduras.

14.6.1 The Contractor shall support troubleshooting, repairing, and changing of cable pairs, and for mission related tasks.

14.7 Long-haul Backbone Circuits. Local Foreign National personnel are authorized to support DISA backbone circuits. DISA services are provided via fiber optics and satellite terminals. The Contractor shall provide a Node Site Coordinator (NSC) to assist DISA with troubleshooting and

testing during outages and Preventive Maintenance (PM) procedures. Should a circuit go down, DISA will alert the DISA RNOSC, who will immediately notify the Node Site Coordinator (NSC) for action.

14.7.1 The Contractor shall provide a primary and alternate point of contacts with Secret Security Clearances to coordinate DISA requirements. The points of contact must be familiar, and have the knowledge to order long haul circuits and services thru the DISA Direct Order Entry (DDOE) system or the equivalent, and perform queries/searches in the Telecommunications Certification Office Support System (TCOSS). General NSC administrative duties, requirements, and procedures are listed in DISA Circular DISAC 310-55-9.

14.7.2 Commercial Lease Circuits. The Contractor shall provide personnel to coordinate, order, account for, and administer local circuits with commercial carriers. Prior to entering into any new leases, the Contractor shall coordinate and get approval from the COR.

14.8 Wireless Infrastructure/Wireless Services. The Contractor shall provide local and international wireless voice and data services to Soto Cano Air Base personnel for official business.

14.8.1 Wireless Voice and Data Services. The Contractor shall coordinate with local vendors to provide wireless voice and data services to Soto Cano Air Base personnel. This includes maintaining Blackberry (or equivalent) service and providing Blackberry (or equivalent) trouble resolution to the Soto Cano Air Base users.

14.8.2 Wireless Intrusion Detection Systems (WIDS). The Contractor shall provide O&M support to the WIDS systems installed throughout Soto Cano Air Base in support of Program Managed (PM) Systems or as required by the Government.

14.8.3 The Contractor shall assist during modernization efforts and hardware/software upgrades of the wireless networks.

14.9 Tactical Communications. The Contractor shall provide O&M support to the JTF-B Tactical Satellite Systems. The Contractor shall maintain and repair the deployable systems used for contingencies and exercises located anywhere in the USSOUTHCOM Area of Focus (AOF). The systems can process classified and unclassified data, DSN, voice-over IP, and VTC capabilities. Current International Maritime Satellite (INMARSAT) terminals are Broadband Global Area Network (BGAN) and Global Rapid Response Information Packages (GRRIP) Very Small Aperture Terminals (VSATs).

14.10 Public Address (PA) System (Giant Voice). Local Foreign national personnel are authorized for Public Address (PA) requirements. The Contractor shall provide maintenance for the existing stationary and portable PA systems, including both outdoor and indoor systems

installed throughout the installation. This also includes future systems added on the installation. The stationary public address system consists of base and auxiliary input devices, cable, and speaker systems. The speaker systems are used for U.S. military announcements.

14.10.1 The Contractor shall administer and maintain existing interoperability between the telephone system and Giant Voice siren systems.

14.10.2 The Contractor shall maintain mobile PA systems. The Contractor shall train users and keep track of the mobile PA systems for official ceremonies and events.

14.10.3 The Contractor shall coordinate and conduct monthly voice tests on the stationary PA system, after receiving authorization from the Honduran Air Force Base Commander, and the results shall be documented in the appropriate service logs.

14.11 Radio Equipment. The Contractor shall provide maintenance service and repair for all tactical radio systems utilized in Soto Cano Air Base, both in garrison and in support of contingency exercises (to include all associated components of hardware and software) such as: AN/PRC-117F(V)(C), Single Channel Ground and Airborne Radio Systems (SINCGARS), Tactical and Non-Tactical High Frequency (HF) radios, to include Very High Frequency(VHF)/Ultra High Frequency(UHF) and Land Mobile Radio(LMR) systems such as: Motorola XTS-5000 or its equivalent and its ancillary support devices. Note: This excludes unique Radio, Radar, and Meteorological Navigation equipment in support of Air Traffic Control (ATC) functions.

14.11.1 Local Foreign National Contractor personnel are authorized to service the UHF/VHF LMR antennas and power requirements. The Contractor shall maintain all UHF/VHF radios/devices, peripheral devices, infrastructure, and repeater systems to include installation/de-installation, relocation, programming and all associated components of hardware, and software. The Contractor shall maintain the currently installed GFE repeater system to provide Soto Cano Air Base personnel operational repeater communications within Soto Cano Air Base, Tegucigalpa, and surrounding areas.

14.11.2 The Contractor shall provide radio operator training for Soto Cano Air Base personnel.

14.11.3 The Contractor shall ship, receive, and track items requiring manufacturer-level support for repair, and shall upgrade, retrofit, and provide warranties for associated hardware and software.

14.11.4 The Contractor shall recommend upgrades, utilizing state-of-the-art equipment, to the existing system's baseline for Government approval.

14.11.5 The Contractor shall provide maintenance service within 4 hours of notification from the JTF-B J6 Staff or designated Government representative to correct, repair, or replace a nonfunctional repeater and bring the site back into operational status.

14.11.6 The Contractor shall immediately notify the JTF-B ACOR of all delays with the restoration of repeater service. Immediately is defined as no more than one hour after it becomes apparent that there will be a delay in restoring the repeater service.

14.11.7 The Contractor shall maintain GFE Uninterruptible Power Supply systems for each repeater location.

14.11.8 The Contractor shall coordinate with appropriate ACOR to determine the optimum number of repeaters and repeater site locations in order to provide a repeater system that meets the communications needs at Soto Cano Air Base. If additional coverage is required, the contractor shall be required to install/de-install additional repeaters or to move an existing repeater to an alternate location.

14.11.9 The Contractor shall establish land and tower space leases for the repeater system upon expiration of current leases. The COR, with input from JTF-B, has final approval of site location and installation. Prior to entering into any new leases, the Contractor shall coordinate and get approval from the COR. The current system uses Motorola XTS-5000 radios and Quantar repeaters, allows securable operation, and is Digital Private Line (DPL) capable.

14.11.10 The Contractor shall test the repeater system coverage once a month and provide a written report of the results to the ACOR.

15. Frequency Spectrum Management. The Contractor shall provide a primary and alternate Frequency Manager (FM). The Contractor shall coordinate with the Government to ensure appointed individuals attend the two-week FM course to become proficient with Spectrum 21 and receive orientation from USSOUTHCOM J6 Frequency Manager, and shall provide a copy of the certificate to the ACOR upon completion. Upon ACOR request, the Contractor shall prepare and submit frequency assignment proposals for Soto Cano Air Base. The Contractor shall assist in working with Honduran and USSOUTHCOM authorities to resolve any frequency interference problems that may arise.

15.1 The Contractor shall provide spectrum coordination support to each unit, organization, or activity authorized the use of frequencies in accordance with (IAW) applicable Army Regulation (AR) 5-12 and local supplemental regulations and procedures.

15.2 The Contractor shall support the Government Spectrum Manager to assign and update authorized radio frequencies or submit requests to the appropriate frequency management office to support mission requirements and external agencies operating in the local spectrum.

15.3 The Contractor shall implement guidance from the USSOUTHCOM J6 FM in support of operations & maintenance of DD Form 1494, Frequency Assignments, and site license surveys for the Soto Cano Air Base areas.

15.4. The Contractor shall assist the Installation Safety Officer with required Radiation Hazard Surveys and maintain copies of all documentation, including Final Reports and implement recommended safety measures identified in the Final Report. The Contractor shall comply with OSHA standards.

15.5 The Contractor shall maintain a current listing of Frequency Assignments for Soto Cano Air Base and provide to the JTF-B J6 and the USSOUTHCOM Spectrum Manager upon request.

16. Crash Conference. Local Foreign National personnel are authorized to support the crash conference systems. The Contractor shall provide and maintain the existing circuits and phones that connect to the crash conference systems to include connectivity and/or inter-connectivity for systems within Soto Cano Air Base. The contractor is not responsible to Operate and Maintain (O&M) main crash conference system within Soto Cano Air Base. The Contractor shall only be responsible to operate and maintain the secondary crash system (Sonexis) that is part of the Telephone Switch MSU in A-47. The Contractor shall modify existing crash conference circuits upon approval from the ACOR.

17. Honduran Telecommunications. Local Foreign National personnel are authorized to support local Honduran Telecommunications. The Contractor shall provide telecommunications support to selected institutions in Honduras. The Contractor shall be required to support or expand additional capability at the Government's request

17.1 Honduran Local Service Provider Circuits. The Contractor shall support Honduran circuits provided by a commercial local carrier to interconnect the Soto Cano and MILGRP telephone switches to the Public Switch Telephone Network (PSTN). The Contractor shall assist and coordinate with the local carrier provider to maintain the following circuit connectivity within Honduras:

One (1) Clear-channel E-1 between Soto Cano Air Base MSU and the MILGRP, Tegucigalpa RSU.

One (1) Direct Inward Dialing)/(Direct Outward Dialing(DID/DOD) E-1 provided by the local carrier between the MILGRP Tegucigalpa RSU to the Tegucigalpa Commercial Central Office.

One (1) DID/DOD E-1 provided by the local carrier between Soto Cano Air Base MSU and the Comayagua Commercial Central Office.

Note – This requirement may be deleted next year once the MILGRP moves to the new U.S. Embassy.

17.2 Off-Premises Extension (OPX) Lines. The Contractor shall maintain the following leased Off-Premises Extension (OPX) lines in Honduras: one hot line in Toncontin Airport Control Tower, one hot line in CENAMER Facilities in Cerro La Mole, one OPX line in Toncontin Airport Control Tower, three OPX lines in Cerro La Mole, four OPX lines to Toncontin Hernan Acosta Mejia Honduran Air Base, eight OPX lines to the US Embassy in Tegucigalpa, one OPX line to the US Embassy Guest House Transient Personnel Quarters (TPQ), and two OPX lines to the Toncontin Hernan Acosta Mejia HAB to support the US Air Force personnel. In case of failure, the contractor shall coordinate with the commercial service provider to expedite restoral.

17.3 Microwave System. The Contractor shall O&M the GFE Microwave System. The existing microwave system will be used as back-up to the E-1 circuits provided by the local carrier to interconnect the Soto Cano and MILGRP telephone switches to the PSTN.
The microwave system shall also be used to support the Land Mobile Radio (LMR) Network.

17.4 The Contractor shall maintain the data channels required for reporting alarm and status indications to the existing Telephony Management System (TMS) installed in Soto Cano Air Base. Alarm and status indications include environmental, power system, security, and electronic equipment reporting signals. The Contractor shall determine the architecture required to comply with this requirement, and provide recommendations to the COR and JTF-B J6.

17.5 The Contractor shall operate and maintain the remote sites in support of the long haul requirements listed above to include maintaining Air Conditioning backup electrical power, generators, rectifiers, inverters, and eight-hour capacity battery backup systems.

18. Power and Air Conditioning. Local Foreign National personnel are authorized to provide Power and Air Conditioning (AC) maintenance and repair in support of the C4S infrastructure. The Contractor shall maintain the existing AC and uninterruptible backup power system equipment to include: generators, automatic transfer switches (ATS), related wiring and conduit, battery banks, rectifiers, inverter modules, disconnecting devices, and breaker panels at remote locations (i.e., Cerro El Horno, Cerro La Mole, and Security Cooperation Office-Tegucigalpa), and local facilities. Maintenance of generators includes providing fuel and oil. Maintenance shall be in accordance with the manufacturer's recommended preventive maintenance schedule. Annual fuel consumption for these generators is approximately 11,000 gallons per year.

19. Uninterruptible Power Supply (UPS) Systems and Power Inverter/Battery Bank Systems. Local Foreign National personnel are authorized to provide UPS, Battery Bank, and Power Inverter maintenance and repair. The Contractor shall maintain existing UPS, Battery Banks, Inverters, and Rectifiers units that support Soto Cano Air Base C4S telephone infrastructure for the MSU and RSUs, LAN equipment and server farms at remote sites and the main C4 nodes at buildings G-27, K-01, and A-47. The equipment shall be Simple Network Management Protocol (SNMP) manageable for interface with the TMS system.

20. Main Switching Unit (MSU)/Remote Switching Unit (RSU) Battery Backup System. Local Foreign National personnel are authorized to provide MSU/RSU maintenance and repair. The Contractor shall provide operation and maintenance support on the existing and all new and upgraded MSU, RSUs and its related ancillary equipment to include Battery Banks, Inverter, and Rectifier.

21. Information Directory. The Contractor shall publish an online, printable information directory, which will include telephone dialing instructions, telephone use policies, the official mail distribution scheme, with a complete list of office symbols identifying all Soto Cano Air Base Staff sections/Units and postal unit numbers for overseas activities not serviced by the United States Postal Service, and other information deemed pertinent by JTF-B ACOR. Contractor shall designate a point of contact for updates to the information directory. The Contractor shall also provide monthly updates to an online sub-set of the information directory that includes personnel assigned duty title, office telephone, home telephone, mobile numbers, and PO Box number.

22. Official Mail Distribution. The contractor shall maintain and manage Official Mail, Distribution Management and Office Symbols. The JTF-Bravo Mail and Distribution Management Program is a pay-as-you-go program that uses commercial stamps. The contractor shall be appointed as the Soto Cano Air Base Mail Manager and shall provide overall guidance and management of the JTF-Bravo Official Mail Program as defined in AR 25-51. The contractor shall order, secure, and maintain inventories and accounts for U.S. postage stamps and provide quarterly postage usage report using USPS Form 17 to the COR. The contractor shall process all official mail Monday thru Friday except US holidays.

23, The contractor shall accomplish routine COMSEC functions to include: the requisition, receipt, control, shipment, and destruction of COMSEC hardware and software for the command. The contractor shall accomplish preparation of destruction documentation as well as identification and reporting of COMSEC incidents. The contractor shall monitor all handlers of COMSEC material for regulatory compliance and report instances of noncompliance to the supporting COMSEC account. The contractor shall inventory COMSEC material. The contractor shall accomplish inspection of all COMSEC transaction records for trends and problem areas. Contractor will perform onsite Semi Annual Inventory Reports (SAIR) with all persons who are hand receipting COMSEC material. Contractor will document semiannual onsite inspections of local elements and retain them for a period of two years.

24. Black Key COMSEC Distribution Support. The contractor shall support all local elements located on Soto Can Air Base and transitional elements requiring Black Key COMSEC. The contractor shall accomplish Black key procedures to include, operating Data Management Device Power Station (DMD PS) Black key software laptop computer which includes converting black data to CRYPTO and distribution of material to AN/PYQ-10 fill device. The Black key COMSEC support originates from ARSOUTH COMSEC office. Contractor is required to provide

monthly destructions reports via SIPR scanner and updates as required to support daily operations.

Contractor personnel will operate AN/PYQ-10 (SKL) in support of the black key operations which includes Transmission Key Encryption Key (TrKEK) management, electronic key issue, audit trail uploading, and software updating when required.

Contractor will coordinate with the Property Book Officer (PBO) and J4 to ensure all unserviceable CCI devices are exchanged thru the Army ISSP program, to include Direct Exchange and periodic modernization of CCI devices for network operations.

The COMSEC Distribution office supports 10 SUB Hand Receipt (HR) Sections. This number can increase to support new mission requirements. SUB HR Include: A CO, B CO, C CO 228th AVN BN, Flight OPS 228th AVN, S6 228th AVN,J3 JOC, SKYWATCH, VTC, ARFOR S6, J6 COMSEC.

PART 7 - Attachment 23 - Technical Exhibit 23 – JTF-GTMO Unique Services

1. Facilities: The contractor is authorized access to, and use of, US Government facilities at United States Naval Base (USNB) GTMO. Authorized facilities include: Base housing/quarters, commissary (to include rationed items), Military/Base Exchange, military postal system, hospitals and medical clinics, military banking facilities and/or credit unions, and Morale, Welfare, and Recreation (MWR) facilities. All items purchased in US Military Exchanges shall be for personal use, or consumption only and shall not be sold or used for commercial purposes. The Government reserves the right to withhold the privileges from any contract personnel in case of abuse. Access to MWR facilities and services does not extend to MWR facilities, trips, or activities outside USNB GTMO.

2. Use of Government Vehicles: Contractor shall be authorized use of Government-furnished vehicles pursuant to their duties in this PWS, IAW JTF-GTMO's policies. Examples may include access to specifically restricted areas for which pre-specified Contractor personnel require access. A valid stateside driver's license and additional training that will be administered at JTF-GTMO are required to operate a Government vehicle. Government-furnished vehicles are used for official business only.

3. Housing: Contractor personnel shall coordinate the leasing of housing units with U.S. Naval Base (USNB), Guantanamo Bay, Housing Department IAW current, applicable Housing Department procedures, instructions, and regulations. Housing units available for lease include the following appliances: refrigerator/freezer, stove, microwave, dishwasher, and clothes washer and dryer. Provision of these appliances is subject to change. Issuance of these housing units and rental rates are controlled by the Housing Department, building 2295. Contractor personnel shall abide by all Family Housing Instructions, IAW USNS Guantanamo Bay Housing Department.

4. Medical Coverage: The Contractor shall provide medical insurance from an insurance carrier accepted by the USNB hospital. The insurance shall cover the medical and dental needs for Contractors who are assigned to work at USNB GTMO. The insurance shall also include provisions to cover the costs of emergency medical evacuation from JTF-GTMO if so ordered by USNB hospital authorities. The Contractor shall be responsible and shall ensure that Contractor personnel have the required vaccinations and immunizations required by USNB. Medical services at USNB hospital are limited, and the Contractor shall ensure personnel assigned to work at JTF-GTMO receive a pre-deployment physical/screening for pre-existing medical conditions requiring treatment not available at USNB GTMO. The Contractor shall pre-coordinate with the COR/USNB GTMO health care facility to determine what type medical insurance is acceptable.

4.1 Medical Requirements:

4.1 Contractor personnel shall obtain the vaccinations and immunizations required by local hospital prior to arriving in GTMO. The Contractor shall pre-coordinate with the COR/USNB GTMO healthcare facility to determine the vaccination/immunization requirements: http://www.jtfgtmo.southcom.mil/xWEBSITE/newcomers/newcomers.html.

4.2 Medical services at GTMO hospital are limited. Contractor personnel shall obtain a physical screening for pre-existing medical conditions prior to arriving at GTMO to ensure proper medical treatment can be administered. The Contractor shall pre-coordinate with the COR/USNB GTMO healthcare facility should questions arise regarding GTMO health services provided:
(https://www.cnic.navy.mil/guantanamo/InstallationGuide/GTMOEntryClearanceInformation/index.htm)

4 Contractor Standards of Conduct

4.1 In accordance with DoD regulation 500.7, Standards of Conduct and 18 U.S.C. 1382 (1972), the installation commander has the authority to bar individuals from the installation. The removal from the job site or dismissal from the premises shall not relieve the Contractor of the requirement to provide sufficient personnel to perform the services as required by this PWS. The Government will not reimburse the Contractor for travel and other expenses associated with the removal of personnel.

4.2 The Government reserves the right to require the Contractor to remove from the job site any employee working under this Task Order for reasons of suspected misconduct, a suspected security breach, or suspected to be under the influence of alcohol, drugs, or any other incapacitating agent. Contractor personnel shall be subject to dismissal from the premises upon determination by the COR that such action is necessary and is in the best interest of the Government.

4.3 Contractor personnel are not authorized to carry or possess firearms while stationed in GTMO.

5 Joint Detainee Information Management System (JDIMS): The following requirements are in addition to those covered elsewhere in the main PWS.

5.1. The contractor shall follow the Software Engineering and Integration guidelines outlined in paragraph 5.1.9 and associated subparagraphs of the PWS for modifications and updates to the JDIMS application.

5.2. The Contractor shall operate 4 instances of JDIMS. The JDIMS instances are: one for training, one for development, and one for live operations. The fourth site will be a JDIMS

mirrored site on the JWICS network, which shall be synchronized with the JDIMS SIPRNET production system on a weekly basis, or as directed by the ACOR.

5.3. Due to the mission critical aspects of JDIMS, the contractor shall have dedicated personnel (i.e. not share with other tasks) to complete the following functions.

- Project management
- Server Systems Administration
- Database Administration
- Application Development
- Documentation
- Training

5.4. Reserved

5.5 The Contractor shall initiate and complete efforts to ensure compliance of the JDIMS application with USSOUTHCOM SIE Policy within 2 years of assumption of responsibilities for JDIMS.

5.6 DIMS Sustainment Support (DSS). The Contractor shall provide Hoteled Services Support for DIMS. The Contractor shall assist with DSS system operations as required.

5.7 Training. The Contractor shall provide the following Training Services.

5.7.1 JDIMS Training.

The Contractor shall develop a Training Plan (TP) that identifies training method(s), approach(s), frequency, proficiency level measurement, objectives, standard, etc. The draft training plan shall be submitted within 30 days after assumption of JTF-GTMO responsibilities approval prior to use. The final training plan shall be submitted within five (5) working days when changes are made thereafter. (See Deliverable 97, Attachment 1)

5.8. Land Mobile Radio Training

The Contractor shall provide training support for Land Mobile Radio System (LMRS).

5.9. Radio Maintenance. The Contractor shall provide installation, operations, and maintenance support to ensure at 100% availability of radios.

5.10 The Contractor must comply with the Unified Facilities Criteria (UFC) guidelines.

5.11 Land mobile radio networks, radios, to include configuration of repeaters. The contractor will maintain a current inventory of all radios and repeaters. The inventory list shall be available to the ACOR at all times. The Government utilizes an LMR trunking system.

5.12. Frequency Management Support.

The Contractor shall coordinate JTF-GTMO spectrum supportability requirements with the USSOUTHCOM Frequency Manager and the GTMO Naval Station Installation Frequency Manager. The Contractor shall implement guidance from the USSOUTHCOM J6 FM in support of operations. The Contractor shall accomplish maintenance of DD Form 1494, Frequency Assignments, and site license surveys for the JTF areas.

5.12.1 EMI Investigations

The Contractor shall accomplish investigative reports of Electromagnetic Interference (EMI) from JTF supporting units and commands and elevate preliminary assessment of EMI to ACOR leadership with request for USSOUTHCOM FM resolution assistance if necessary.
The Contractor shall assist the Installation Safety Officer with required JTF-GTMO Radiation Hazard Surveys and maintain copies of all documentation, including Final Reports and implement recommended safety measures identified in the Final Report. The Contractor shall make recommendation to comply with Occupational Safety and Health Administration (OSHA) standards.

5.12.2. Frequency Assignments

The Contractor shall maintain a current listing of Frequency Assignments for JTF-GTMO. The Contractor shall maintain current JTF-GTMO frequency usage plans to ensure that local frequency restrictions are honored. The Contractor shall monitor use of the JTF-GTMO spectrum-dependent systems to ensure they are operated within parameters of frequency licenses. The contractor shall report if there is a requirement to operate beyond parameters of the licenses and help obtain prior authorization from USSOUTHCOM Spectrum Manager.

5.12.3 The Contractor shall Monitor JTF-GTMO spectrum-dependent equipment and report problems with operations or maintenance to JTF GTMO J6 leadership within one hour of identifying the problem.

5.12.4 The Contractor shall ensure JTF-GTMO assigned frequencies are used and report any spectrum-dependent systems that are not operated in accordance with parameters authorized by the Frequency Assignment process.

5.12.5 The Contractor shall accomplish an annual review of JTF-GTMO Site-Licenses to JTF-GTMO J6 CM. The Contractor shall review all licenses to determine currency. The J6 Director/COR will provide format and context for accountability log.

5.12.6 The Contractor shall participate in all planning activities that involve new spectrum-dependent systems, or frequencies.

5.13 The Contractor shall assist with Voice over Internet Protocol (VoIP) implementation upon direction of the ACOR.

NOTE: For the purposes of the JTF-GTMO Frequency Manager Responsibilities, JTF-GTMO implies the JTF, Office of Military Commission (OMC), and any directly attached, or supporting units or commands. Frequency Management support for NAVSTA GTMO may be outside the scope of the Contractor and the authority of the JTF-GTMO J6. Additionally, Electromagnetic Interference (EMI) deconfliction for the JTF-GTMO will be focused only on JTF-specific areas such as the Camp Bulkeley, the detainee camps, Expeditionary Legal Center, Media Operations Center, and Camp Justice. Other temporary/permanent sites designated by the JTF-GTMO/J6 may be required as mission dictates. Spectrum Management for NAVSTA GTMO must be handled through USNB channels. However, the JTF-GTMO Frequency Manager must coordinate with the NAVSTA GTMO Installation Frequency Manager on a routine basis for frequency.

5.14 The Contractor shall provide Office of Military Commission – Office of the Secretary of the Defense with the following TS SCI-required VTC support.

5.14.1 The Contractor shall assist with all phases of the courtroom technical operations, to include maintaining official and unofficial transcription software, auxiliary location support, and current and future Closed Circuit Television (CCTV) infrastructure support.

5.14.2 The Contractor shall provide courtroom and ancillary courtroom systems support and expert technical consultation, which include operators and technicians for satellite, data, VoIP and audio/video transmissions.

5.14.3 Contractor responsibilities shall include, but is not limited to conception, design, engineering, installation and transmission services, quality service checks, and routine maintenance. The Government requires contractor support that can readily and rapidly accommodate Government request(s) for service or alteration to the courtroom systems (this system suite should be considered as an extension of the larger JWICS network, as it is a JTF-GTMO specific suite); thus the contractor shall maintain the flexibility to accomplish the government's mission. The Contractor shall keep OMC abreast on new and emerging courtroom technologies, and will provide advice, engineering services, and installation of equipment to implement such changes upon approval of COR.

5.14.4 The Contractor Audio/Video Operator/Installer shall be available during court sessions and shall provide operator-level work during court sessions. Additionally, the contractor Audio/Video Operator/Installer shall provide setup assistance to trial counsel, trial judiciary, and other technical staff during court sessions.

5.14.5 The Contractor Audio/Video Operator/Installer shall be tasked to provide assistance directly to the Judge in the area of technology assistance or provide direct assistance to court reporters/ stenographers for audio/video issues that arise during sessions.

5.15 Enterprise Vault:

The Contractor shall be responsible for operating effectively and maintaining the historical, production and Enterprise Vault solutions that comprise the collateral and JWICS after completion of the JTF-GTMO phase-in period. These software solutions serve as a centralized repository for data archived since the inception of the Joint Task Force, Guantanamo and are critical to the legal processing of detainees.

ICPG 704.2 Personnel Security Adjudicative Guidelines for Determining Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information (dated 02 Oct 08) http://www.fas.org/irp/dni/icd/index.html

ICPG 704.3 Denial or Revocation of Access to Sensitive Compartmented Information, Other Controlled Access Program Information, and Appeals Processes (dated 02 Oct 08) http://www.fas.org/irp/dni/icd/index.html

ICPG 704.4 Reciprocity of Personnel Security Clearance and Access Determinations (dated 02 Oct 08) http://www.fas.org/irp/dni/icd/index.html

ICD 503 Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation (dated 15 Sep 08) http://www.fas.org/irp/dni/icd

ICD 705 Sensitive Compartmented Information Facilities (dated 26 May 10) http://www.fas.org/irp/dni/icd/index.html

ICPG 705.1 Physical and Technical Security Standards for Sensitive Compartmented Information Facilities (dated 17 Sep 10) http://www.fas.org/irp/dni/icd/index.html

ICPG 705.2 Standards for the Accreditation and Reciprocal Use of Sensitive Compartmented Information (dated 17 Sep 10) http://www.fas.org/irp/dni/icd/index.html

DCID 6/9 Physical Security Standards for Sensitive Compartmented Information Facilities (dated 18 Nov 02) http://www.fas.org/irp/offdocs/dcid.htm

DCID 6/4 Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information (02 Jul 98) http://www.fas.org/irp/offdocs/dcid.htm

6. SPOT - Synchronized Pre-deployment and Operational Tracker (SPOT) System. The Contractor shall register before deployment and maintain all data for all personnel that will be

performing on-site in GTMO. The Contractor shall use the Synchronized Pre-deployment and Operational Tracker (SPOT) web-based System at http://www.bta.mil/products/spot.html, to enter and maintain the data. Registration shall be completed no later than 10 business days after contract award. The Contractor shall submit written evidence of SPOT registration for all personnel performing on-site to the contracting officer and the COR no later than 30 calendar days after award.

7. Defense Base Act (DBA) Insurance Coverage. Pursuant to the War Hazards Compensation Act (WHCA) and Defense Base Act (DBA) FAR clause, DBA insurance coverage is mandatory for contractor personnel that will be performing on-site in Guantanamo Bay, Cuba. The Defense Base Act provides workers' compensation protection to civilian personnel working outside the United States on US military bases or under a contract with the U.S. Government for public works or for national defense. The Contractor shall (a) provide before commencing performance under this Task Order, such workers' compensation insurance or security as the Defense Base Act (42 U.S.C. 1651, et seq.) requires and (b) continue to maintain it until performance is completed. Information on Defense Base Act can be found at www.dol.gov/owcp.

a. The contractor shall submit written proof of DBA insurance during the JTF-GTMO Phase-In Period and no later than 30 calendar days after assumption of responsibilities for JTF-GTMO. Failure to comply with this requirement may result in termination of contract, and carries penalties assessed by the Department of Labor.

b. DBA Proof of Insurance: Contractor shall provide a policy of Defense Base Act Workers' Compensation to the Contracting Officer. The DBA requirement also applies to all subcontractors performing under this PWS. If a subcontractor is performing work under this PWS, the Contractor shall provide evidence of subcontractor's DBA insurance to the Contracting Officer. Absent submission of a subcontractor's DBA policy, the Contractor is required to provide the coverage for the subcontractor's personnel and show proof of insurance. Insurance must be obtained from a provider on the list at http://www.dol.gov/owcp/dlhwc/lscarrier.htm. Purchase of DBA insurance from any provider not on the approved list means that the contractual requirements of FAR 52.228-3 are not met. If the expiration date of the policy is before the performance ends, then prior to expiration, the Contractor shall provide a new policy or renewal of existing policy to cover the performance to the ending date of performance.

c. The Contractor shall keep posted in a conspicuous place in and about its place of business either a typewritten or printed notice on Forms LS-241 (Notice to Personnel) or LS-242 (Notice to Personnel for Self-Insured Employers). Such notice must also contain the name and address of the employer representative to who notice of injury is given, and the carrier, if any, with whom the employer has secured payment of compensation and the date of the expiration of the policy. Posted notice shall be written in the language of the personnel. Additional information is available at http://www.dol.gov/owcp/dlhwc/lsdba.htm.

8. Relocation. The Contractor is responsible for the relocation and shipment of household goods (HHG). The following are the maximum amounts the Contractor will be reimbursed per contracted position by the Government and is provided for price proposal purposes: personnel working on-site under the contract to and from the Naval Station Guantanamo Bay, Cuba. The following are the maximum amounts the contractor will be reimbursed per contracted position by the Government and is provided for price proposal purposes:

(a) HHG weight allowance shall not exceed 10,000 lbs round trip for accompanied tour and 6,000 lbs round trip for unaccompanied tour.

(b) The Government will reimburse the round trip cost to transport one (1) privately owned vehicle (POV) for each Contractor employee from home of record to Jacksonville, Florida. This cost is capped at $5,000 round trip. The Contractor will not be responsible for charges incurred by the barge that transports the POV from Jacksonville, Florida to JTF-GTMO.

c) Contractor airfare from home of record to Naval Station Guantanamo Bay shall not exceed $2,500 round trip.

(d) Storage fees for HHG arriving JTF-GTMO off of the barge awaiting delivery to the contractor's housing unit shall not exceed $1,500 round trip.

(e) The Government will provide up to ninety (90) days of temporary lodging per employee upon initial arrival at JTF-GTMO while waiting for Government housing assignment or delivery of Household Goods. The Government will not reimburse for more than $50.00 per night while occupying temporary lodging.

9. Turnover of Personnel: See paragraph 1.6.20.5 Personnel Vacancy for JTF-Bravo, JTF-GTMO, or SCOs

10. Housing. The Government will provide housing (based on availability) for the Contractor's use. The housing units are reserved for use by accompanied or unaccompanied personnel only. Housing will be assigned as follows: accompanied personnel by family composition with maximum family size of three (3) dependents; unaccompanied personnel assignment will be made based on a minimum of one person per bedroom. Note the Contractors with greater than 3 dependents will only be assigned housing using 3 dependents as the planning factor. If house sharing, accompaniment by dependents will not be allowed. Contractor personnel will be required to provide all household furnishings. The Government will provide family housing units with the following appliances: refrigerator, stove, dishwasher, microwave, washer, and dryer. Housing may provide temporary loaner furniture for up to 90 days, depending on availability. No extensions will be granted. All furnishings other than the listed appliances in paragraph 4.2 of this PWS will be provided by the contractor following the initial 90-day loaner period. Issuances of these housing units and rental rates are controlled by the Housing Department, building 2295,

phone 011-53-99-4172/4174. Contractor personnel shall abide by all Family Housing instructions, which are not part of this Task Order but available upon request. Contractors will pay rent under the Fair Market Rental (FMR) Program and these rates are available upon request. Rental rates DO NOT include utility costs. The Government is not responsible for, and will not pay for damages to occupant quarters caused by the negligence of the Contractor occupants.

Estimated Housing Rental Rates. All rent is due in advance. No personal checks accepted. The below rates are based on current administration of shelter rent, and is for informational purposes only:

Rental Rates for housing:

# Bedrooms/	# Baths Rent
1 bedroom/1 bath	$737
2 bedroom/1 bath	$737
2 bedroom/1.5 bath	$788
3 bedroom/1 bath	$883
3 bedroom/2 bath	$976
4 bedroom/2.5 bath	$1,166

All family housing units are equipped with electric and water meters. Contractors will be billed for actual utility usage. Utility expenses will be capped at the monthly utility rates listed below:

# Bedrooms/# Baths	Monthly Utilities Cap
1 bedroom/1 bath =	$900.00
2 bedroom/1 bath =	$900.00
2 bedroom/1.5 bath =	$975.00
3 bedroom/1 bath =	$1,025.00
3 bedroom/2 bath =	$1,050.00
4 bedroom/2.5 bath =	$1,050.00

The Government will not pay for any utility expenses exceeding the listed monthly utility rate caps.

11. The Government will provide tuition reimbursement for Department of Defense Dependents Schools (DODDS) to cover tuition for up to 20 students on an accompanied basis. School tuition is capped at $24,419.00 per child for a maximum of 20 students. The Contractor dependents may attend DODDS Schools on a cash reimbursable basis at the prevailing rates. Current rate for the school year are as follows:

Grades	Cost Per Student Per Year

Sure Start Programs	$11,004.00
Kindergarten through Grades 6	$22,008.00
Grades 7 through 8	$23,172.00
Grades 9 through 12	$24,336.00

12. Government Rental Vehicles: The Government will authorize the Contractor up to three (3) rental vehicles to utilize for Government purposes only. The ACOR shall authorize vehicle usage. Fuel shall not be reimbursed. Rental vehicle expenses will be capped at $700 per vehicle, per month.

PART 7 - Attachment 24 - Technical Exhibit 24 – Software Engineering and Integration

See separate Software Engineering and Integration (SEI) Policy

PART 7 - Attachment 25 - Technical Exhibit 25 – Defense Cyber Operations and NetOps Tool Sets

HQ USSOUTHCOM & ADR - NetOps Toolsets		
Location	Primary Tool	Modules / Use
HQ USSOUTHCOM - 525th Signal Co.	Heat - Trouble Ticketing System	Tracking & Reporting
	525th's WhatsUpGold	HQ's Network Monitoring
	HBSS	Network Security Monitoring & Management
	WEBSense	Internet Monitoring
	SCOM	
	Cisco Work Prime	
	Cisco NCM	
	Cisco ASDM	Manage Firewalls
	SPLUNK Netscout	
	IBM Site Protector	Manage IPS's
	Fidelis	
	Snort Sensor	
	ARBOR	
	ENCASE	Security Incident Response
HQ USSOUTHCOM - JNCC	DISA's iNMS	Network Monitor
	DISA's ITSM (Remedy)	Trouble Ticketing System
	TCSC's Solarwinds	Network Monitoring - SCOs
	525th's WhatsUpGold	HQ's Network Monitoring
	NETCOM's Spectrum Management	JTF-BRAVO & JTF-GTMO Network Monitoring
	NETCOM's ITSM (Remedy)	NIPR Only - Trouble Ticketing System
	525th's /TNCC's Heat-Trouble Ticketing Syster	Tracking & Reporting
JIATF-S	Solarwinds Suite	Server & Application Monitor
	Putty	Virtualization Manager
	Cisco ASDM	Storage Manager
	DISA's HBSS	Network Performance Monitor
	Proventia/SiteProtector	Network Configuration Manager
	Oradar	Netflow Traffic Analyzer
	SecurityCenter	Engineer's Toolset
		User Device Tracker
		Log & Event Manager
		Firewall Security Manager
		Alert Manager
JTF-BRAVO	Cisco ASA Firewalls	
	Websense Web Traffic	NIPR Only
	IBM Proventia	IDS/IPS
	SNORT IDS Device	Monitored by RCERT-South
	CA Spectrumgt/E-Health	Non-Operational ATT
	Enterprise Service Management System	NETCOM's (ARMY) Trouble Ticketing System (Remedy)
JTF-GTMO	CISCO Prime LAN Mgt Solution (LMS)	
	MS Admin Tool Suite	Remote Desktop/RDP, Service Mgr, Active Dirctory etc
	CA Spectrumgt/E-Health	Remote Network Monitoring
	CA Unified Svc Desk Mgr	USD Ticketing System
	MS Center Configuration Mgr (SCCM)	
	MS Windows Server Update Services (WSUS)	
	MS System Center Operations Mgr (SCOM)	
	Orion Solarwinds	Network Monitoring
	VmWare vCenter	Virtualization & Server Management
	MS NetbackUp	
SOCSOUTH	SCRIPTLOGIC	3rd Party SW
	DoDWSUS	Windows Patching
	HBSS	Network Security Monitoring & Management
	Solarwinds	Network Monitoring & Management
	Snort Sensor	RCERT-S"s Tool
	Proventia/SiteProtector	RCERT-S"s Tool
	WEBSense	Internet Monitoring

PART 7 - Attachment 26 - Technical Exhibit 26 – Generic Network Diagram

Figure 1 – Generic Network Diagram – Any Given Network

All Are Active Directory Based

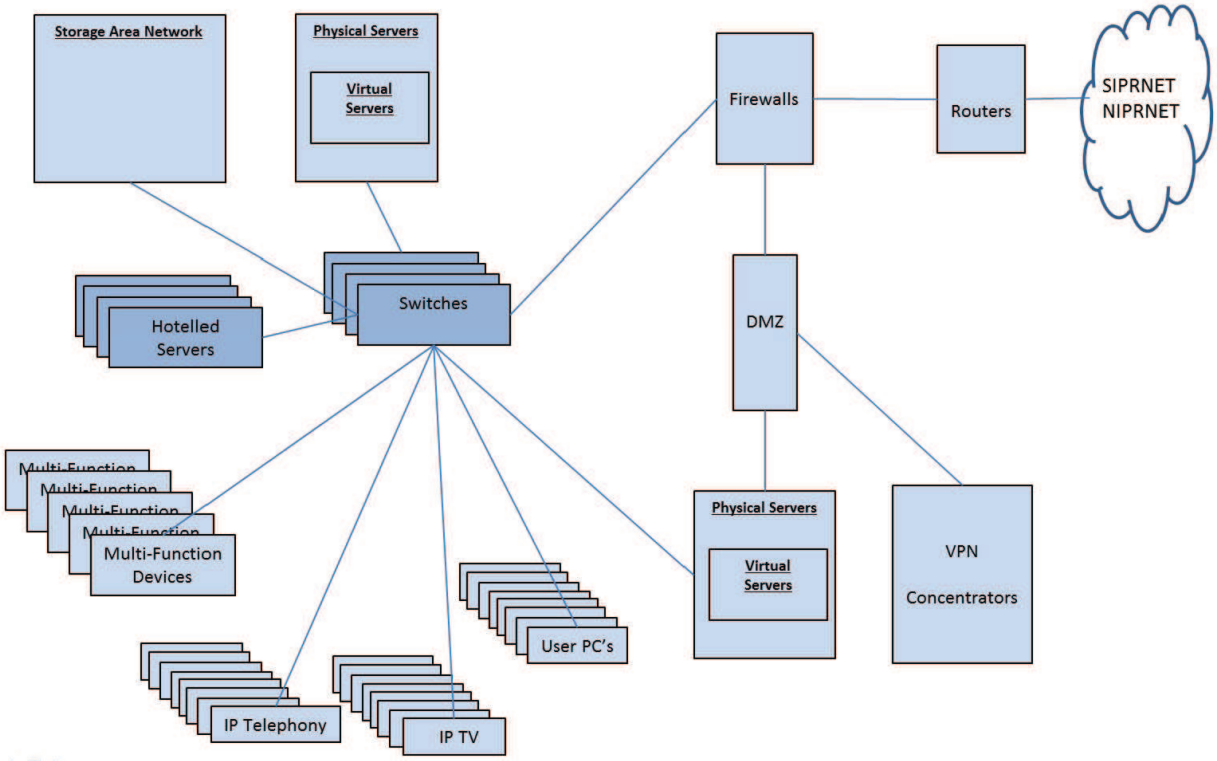

Figure 2 – A simplified depiction of all existing network environments

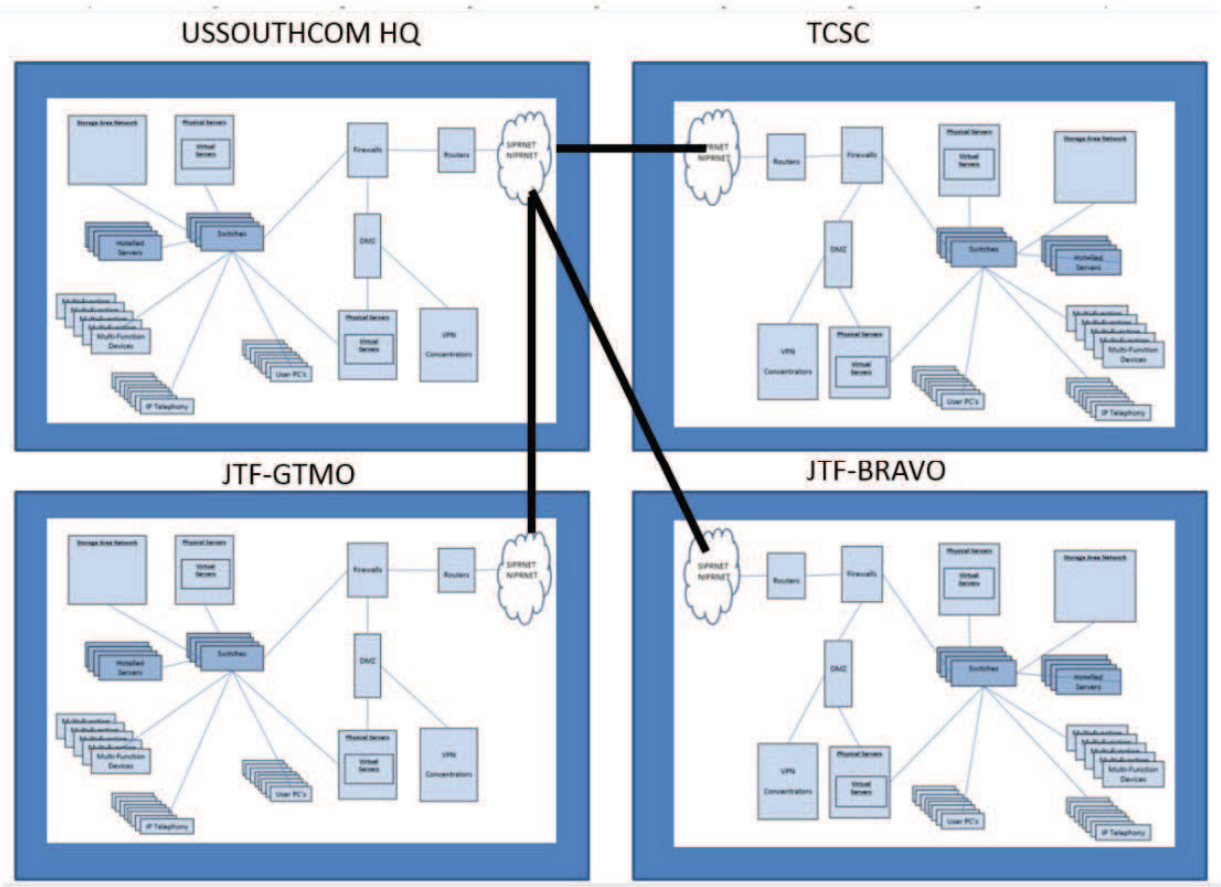

Figure 2 – Simplified depiction of Deprecation of SOUTHCOM Networks – A step prior to Moving to the JIE Cloud Computing based Concept

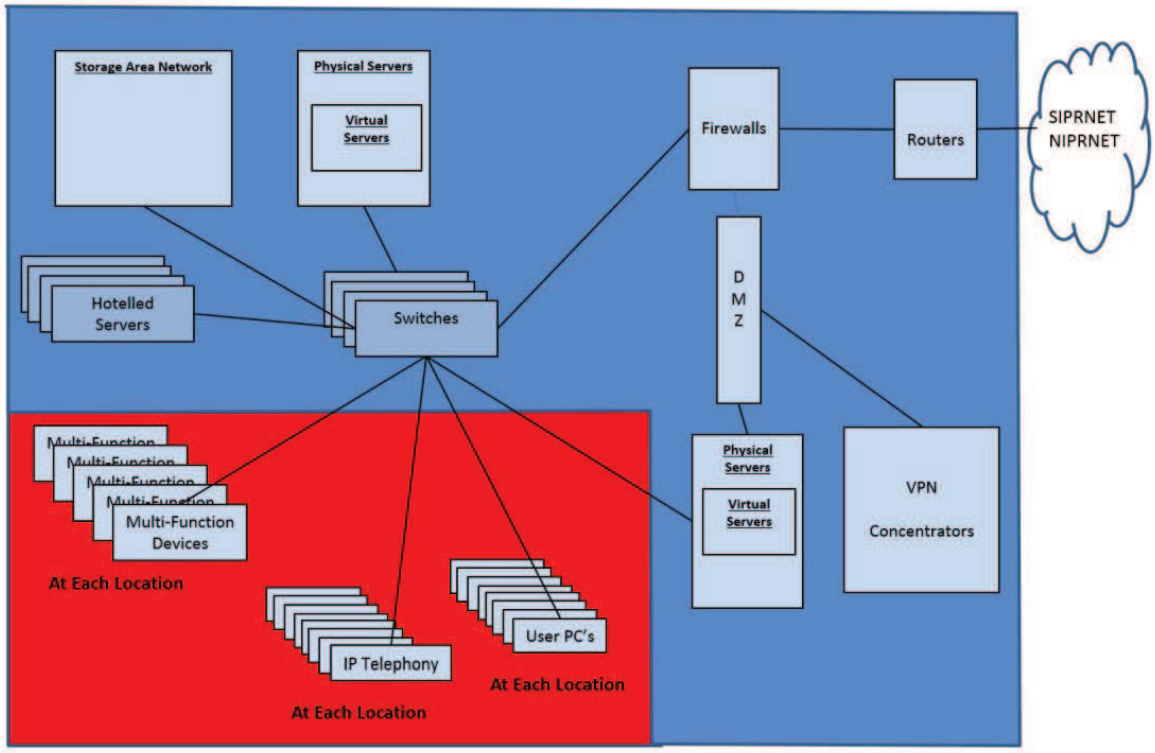

Figure 3 - Simplified depiction of the JIE Migration – All Systems in Blue are a US SOUTHCOM HQ Systems in Red are at USSOUTHCOM HQ, JTF-Bravo, JTF-GTMO and the 26 Embassies in USSOUTHCOM AOR

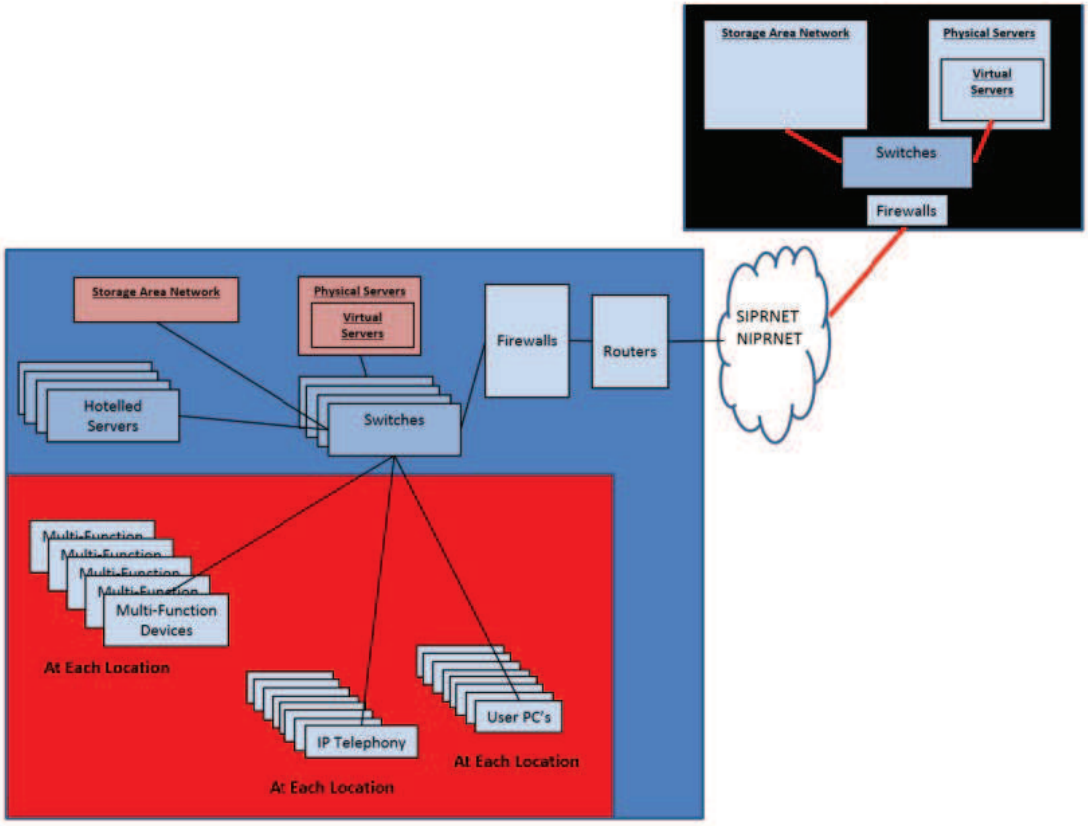

Figure 3 represents the collapse of networks and implementation of the new requirement for JIE. All applications are hosted in the DoD cloud, whereas in Figure 2, SOUTHCOM HQ maintains all applications locally

Example of a Script on One Network in the AOR

The scripts are run each morning from one of the management servers and from the file server on both NIPR and SIPR. The script will touch each server and gather the server health information; space on drives, memory utilization, etc. It will use this information to create a summary page that, in table format, for each server scanned where the overall health of the server can be quickly viewed. The other portion of the script will take the contents of the major Windows event logs (Application, Security, and System) and create a page where they can be viewed in table format according to server and log. The events are color coded according to severity where the administrator can easily view them and take any necessary action accordingly. The logs are also emptied and copied to each respective server so they can be referenced, if necessary, at a later date.

PART 7 - Attachment 27 - Technical Exhibit 27 – Performance Requirements Summary

The Contractor Performance requirements are summarized into performance objectives that relate directly to mission essential items. The performance threshold briefly describes the minimum acceptable levels of service required for each requirement. These thresholds are critical to mission success. Task Order surveillance will be performed by the COR and appropriate ACORS.

Performance Objectives	Performance Standards	Performance Threshold	Methods of Surveillance	Impact on Contractor Payments or Other Impact
PRS #1 Accomplishment of Planning, Designing, Phase – In of work responsibilities or Transition New Technical/Operational Capabilities References: IT Service Strategy, (PWS 5.1.1) IT Service Design (PWS 5.1.2) IT Service Transition (PWS 5.1.3)	Technical performance. Meet the approved technical requirements, technical design and technical performance. Schedule. Meet the approved capability delivery schedules (Applies to JIE or New Capability CLINs) Timeliness of deliverables. Provide required documentation and reports in accordance with schedules. Resource control and Management. Meet milestones or complete deliveries within approved labor hours and labor costs. (Time and Materials CLINs Only)	For New/Modified Capabilities, Passes Acceptance Testing and conforms to Functional and Physical Configuration Audits. Within +/- 15% of the agreed schedule Within +/- 15% of the agreed schedule Within +/- 10% of agreed resources (labor hours or labor costs for Time and Material CLINs)	100% Review of Deliverables	Positive Comments and Ratings or Negative comment and ratings respectively for successful or unsuccessful performance. Possible exercise of options for successful performance. Possible decision to not exercise future options for unsuccessful performance.

PRS #2 Meet Performance Requirements for All Services References IT Service Operations (PWS 5.1.4)	Meet performance requirements for all services identified in attachment 9 Timeliness of deliverables. Provide required documentation and reports in accordance with schedules.	Availability in accordance with attachment 9 Within +/- 15% of the agreed schedule	100% Review of Deliverables	Positive Comments and Ratings or Negative comment and ratings respectively for successful or unsuccessful performance. Possible exercise of options for successful performance. Possible decision to not exercise future options for unsuccessful performance.
PRS #3 Ability to Identify Process Improvements or Efficiencies Reference: Continuous IT Service Improvement (PWS 5.1.7)	Timeliness of deliverables. Provide required documentation and reports in accordance with schedules.	Within +/- 15% of the agreed schedule	100% Review of Deliverables	Positive Comments and Ratings or Negative comment and ratings respectively for successful or unsuccessful performance. Possible exercise of options for successful performance. Possible decision to not exercise future options for unsuccessful performance.
PRS #4 Accomplish Software Engineering and Integration Activities Reference	Technical performance. Meet the approved technical requirements, technical design and technical performance.	For SEI Capabilities, Passes Acceptance Testing and conforms to Functional and Physical Configuration Audits.		Positive Comments and Ratings or Negative comment and ratings respectively for successful or unsuccessful performance.

Software Engineering Integration Life Cycle Support Activities (PWS 5.1.9)	Schedule. Meet the approved capability delivery schedules (Applies to JIE or New Capability CLINs) Timeliness of deliverables. Provide required documentation and reports in accordance with schedules. Resource control and Management. Meet milestones or complete deliveries within approved labor hours and labor costs. (Time and Materials CLINs Only)	Within +/- 15% of the agreed schedule Within +/- 15% of the agreed schedule Within +/- 10% of agreed resources (labor hours or labor costs for Time and Material CLINs)	100% Review of Deliverables	Possible exercise of options for successful performance. Possible decision to not exercise future options for unsuccessful performance.
PRS #5 Accomplish IT Systems Support Services Reference: IT Systems Support Services (PWS 5.1.10)	Timeliness of deliverables. Provide required documentation and reports in accordance with schedules.	Within +/- 15% of the agreed schedule	100% Review of Deliverables	Positive Comments and Ratings or Negative comment and ratings respectively for successful or unsuccessful performance. Possible exercise of options for successful performance. Possible decision to not exercise future options for unsuccessful performance.

PRS #6 Accomplish Other Required Support Services in Colombia, JTF-Bravo, and JTF-GTMO Reference: Other Required Support Colombia, (JTF-Bravo, JTF-GTMO) (PWS 5.1.11)	Timeliness of deliverables. Provide required documentation and reports in accordance with schedules.	Within +/- 15% of the agreed schedule	100% Review of Deliverables	Positive Comments and Ratings or Negative comment and ratings respectively for successful or unsuccessful performance. Possible exercise of options for successful performance. Possible decision to not exercise future options for unsuccessful performance.
PRS #7 Accomplish Exercise and Contingency Operations Support Reference: Exercise and Contingency Operations Support PWS Paragraph 5.2.5	Timeliness of deliverables. Provide required documentation and reports in accordance with schedules.	Within +/- 15% of the agreed schedule	100% Review of Deliverables	Positive Comments and Ratings or Negative comment and ratings respectively for successful or unsuccessful performance. Possible exercise of options for successful performance. Possible decision to not exercise future options for unsuccessful performance.

PART 8 - POINTS OF CONTACT

The following Points of Contact should be utilized for this order:

Contracting Officer:

U.S General Services Administration
Federal Acquisition Service (FAS)
ATTN: Charles Ade, Contracting Officer
ITSS Task #: ID02140034
Tel: 347-525-5151
Email: charles.ade@gsa.gov

Contracting Officer's Representative (COR):

General Services Administration
Federal Acquisition Service (FAS)
ATTN: Thomas Corley, Information Technology Manager
ITSS Task #: ID02140034
Building 3305, Suite 106
Picatinny Arsenal, NJ 07806
Tel: 347-752-7302
Email: thomas.corley@gsa.gov

SOUTHCOM COR:

Carlos Garcia, DAC, GS-14
USSOUTHCOM J6 Directorate
9301 NW 33rd Street
Doral, FL, 33172
CM: 305-437-1926/DSN: 567-1926
Fax: 305-437-xxxx
Email: carlos.garcia29..civ@mail.mil

PART 9 - CONTRACT CLAUSES

All clauses contained in the Contractor's Alliant SB contract.

Additionally, the following clauses are incorporated by reference:

52.251-1 Government Supply Sources (April 2012) Additionally, most items acquired under FAR Part 51 authority will be acquired under the Army's CHESS program. In exceptional cases, items may be procured through the Federal Supply Schedule program. Items offered that may be procured using the FAR Part 51 deviation authority allowing contractors to acquire goods using Federal Supply Schedules must be proposed/procured on a T&M/LH basis.
52.246-5, Inspection of Services – Cost Reimbursement (May 2001)
52.246-25, Limitation of Liability-Services (Feb 1997)
52.245-9 Use and Charges (April 2012)(GFE mentioned in PWS to be provided without charge.)
52.245-1, Government Property. (Apri 2015)
52.237-3, Continuity of Services (Jan 1991)
52.232-7 Payments Under Time-and-Materials and Labor-Hour Contracts. (Feb 2007)
52.228-4, Workers' Compensation and War-Hazard Insurance Overseas (April 1984)
52.228-3, Workers' Compensation Insurance (Defense Base Act) (Jul 2014)
52.227-1; Authorization and Consent (Jul 1995)
52.223-10, Waste Reduction Program (May 2011)
52.222-50 Combatting Trafficking in Persons (Mar 2015)
52.219-27 Notice of Service-Disabled Veteran-Owned Small Business Set-Aside (Nov 2011)
52.212-4 Contract Terms and Conditions-Commercial Items (May 2015)
252-251-7000; Ordering from Government Supply Sources (Aug 2012)
252.247-7024, Notification of Transportation of Supplies by Sea (Mar 2000)
252.247-7023, Transportation of Supplies by Sea (April 2014)
252.245–7004, Reporting, Reutilization, and Disposal (Mar 2015)
252.245-7003, Contractor Property Management System Administration (April 2012)
252.245–7002, Reporting Loss of Government Property (April 2012)
252.245–7001, Tagging, Labeling, and Marking of Government-Furnished Property (April 2012)
252.232-7007, Limitation of the Government's obligation (APR 2014) (to be completed at award)
252.228-7003 Capture and Detention (Dec 1991)
252.227-7037, Validation of Restrictive Markings on Technical Data (June 2013)
252.227-7030, Technical Data–Withholding of Payment (March 2000)
252.227-7028, Technical Data or Computer Software Previously Delivered to the Government (June 1995)
252.227-7016, Rights in Bid or Proposal Information (Jan 2011);
252.227-7014 Rights in Non-commercial Computer software and noncommercial computer software documentation (Feb 2014)
252.227-7013, Rights in Technical Data–Noncommercial Items (Feb 2014)

252.225-7987, Requirements for Contractor Personnel Performing in USSOUTHCOM Area of Responsibility (DEVIATION 2014-O0016)(OCT 2014) available at:
http://www.acq.osd.mil/dpap/policy/policyvault/USA004118-14-DPAP.pdf
252.225-7043 Antiterrorism/Force Protection for Defense Contractors Outside the United States (Mar 2006)
252.225-7040 Contractor Personnel Supporting U.S. Armed Forces Deployed Outside the United States (Jan 2015)
252.223-7004, Drug-free Work Force (Sept 1988)
252.211-7007, Reporting of Government-Furnished Property (Aug 2012)
252.211-7003 Item Unique Identification and Valuation (Dec 2013)
252.204-7008; Export-Controlled Items (Apr 2010)
252.201-7000 Contracting Officer's Representative (Dec 1991)
The following clauses are incorporated:

52.217-8 Option to Extend Services (Nov 1999)
The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a Result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor within _60 days.____

52.217-9 OPTION TO EXTEND THE TERM OF THE CONTRACT (Mar 2000)
(a) The Government may extend the term of this Task Order by written notice to the Contractor within __30_ days; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 60 days before the contract expires. The preliminary notice does not commit the Government to an extension.
(b) If the Government exercises this option, the extended contract shall be considered to include this option clause.
(c) The total duration of this Task Order, including the exercise of any options under this clause, shall not exceed 82 months.

PART 10 – Reports in ITSS and INVOICING

Reports in ITSS:

In addition to posting to the USSOUTHCOM SharePoint (or equivalent) repository, the contractor shall post to the ITSS system the Periodic Program Progress, Status and Management Report described as Deliverable #2, within one work day of posting the report to the USSOUTHCOM SharePoint (or equivalent) repository.

Invoicing:

The contractor shall submit invoices electronically by logging into the ASSIST portal (https://portal.fas.gsa.gov), navigating to the order, and creating the invoice for the order.

The Contractor shall submit Requests for Payments in accordance with the format contained in GSAM 552.232-70, INVOICE REQUIREMENTS (SEP 1999), and shall at a minimum include the following information to have the invoice considered proper for payment.

(a) Contract number;

(b) Paying Number: (ACT/DAC NO.);

(c) Applicable CLIN or Sub-CLIN in which the costs were incurred, quantity, unit price and extended price;

(d) If applicable, incurred cost of all approved travel to include name of Government approving official and date approved;

(e) List of all applicable materials and/or services provided under this order to include the part number, nomenclature, quantity, and the unit and extended price;

The Contractor shall include the following statement on all invoices submitted for payment: “The costs and pricing contained within this invoice do not exceed the allowable costs of the applicable Government contract.”

The Contractor shall ensure that all requests for payments are validated, signed and dated by the Contracting Officer’s Representative, identified in Section 13.4, of this delivery order before submitting to GSA for approval and payment. The invoice shall include the following statement. “I, printed name of Government POC, have verified that in a satisfactory manner the items identified have been received or the services have been rendered and I take no exceptions to this invoice.”

The contractor shall submit invoices electronically by logging into the ASSIST portal (https://portal.fas.gsa.gov), navigating to the order, and creating the invoice for the order.

Unless otherwise specified in this delivery order, the Contractor shall forward all originals of correspondence requiring signature to the CO.

Change Log:

Version number	Date issued	Reason for Change	(Reserved)
Baseline 1.0 version	09/28/15	Issued with order.	
Revised 2.0 version	03/08/16	Incorporate MNIS requirement (see para 5.1.10.2.2.)	
Revised 3.0 version	06/07/16	Clarify requirements and correct grammar and punctuation at no cost to either party.	

QUALITY ASSURANCE SURVEILLANCE PLAN (QASP)

1. INTRODUCTION

This quality assurance surveillance plan (QASP) is pursuant to the requirements listed in the performance work statement (PWS) entitled U.S. SOUTHERN COMMAND (USSOUTHCOM) ENTERPRISE INFORMATION TECHNOLOGY SERVICES SUPPORT CONTRACT (EITSSC). This plan sets forth the procedures and guidelines USSOUTHCOM J6 will use in ensuring the required performance standards or services levels are achieved by the contractor.

1.1 Purpose

The purpose of the QASP is to describe the systematic methods used to monitor performance and to identify the required documentation and the resources to be employed. The QASP provides a means for evaluating whether the contractor is meeting the performance standards/quality levels identified in the PWS and the contractor's quality control plan (QCP), and to ensure that the government pays only for the level of services received.

This QASP defines the roles and responsibilities of all members of the integrated project team (IPT), identifies the performance objectives, defines the methodologies used to monitor and evaluate the contractor's performance, describes quality assurance documentation requirements, and describes the analysis of quality assurance monitoring results.

1.2 Performance Management Approach

The PWS structures the acquisition around "what" service or quality level is required, as opposed to "how" the contractor should perform the work (i.e., results, not compliance). This QASP will define the performance management approach taken by USSOUTHCOM J6 to monitor and manage the contractor's performance to ensure the expected outcomes or performance objectives communicated in the PWS are achieved. Performance management rests on developing a capability to review and analyze information generated through performance assessment. The ability to make decisions based on the analysis of performance data is the cornerstone of performance management; this analysis yields information that indicates whether expected outcomes for the project are being achieved by the contractor.

Performance management represents a significant shift from the more traditional quality assurance (QA) concepts in several ways. Performance management focuses on assessing whether outcomes are being achieved and to what extent. This approach migrates away from scrutiny of compliance with the processes and practices used to achieve the outcome. A performance-based approach enables the contractor to play a large role in how the work is performed, as long as the proposed processes are within the stated constraints. The only exceptions to process reviews are those required by law (federal, state, and local) and compelling business situations, such as safety and health. A "results" focus provides the contractor flexibility to continuously improve and innovate over the course of the contract as

long as the critical outcomes expected are being achieved and/or the desired performance levels are being met.

1.3 Performance Management Strategy

The contractor is responsible for the quality of all work performed. The contractor measures that quality through the contractor's own quality control (QC) program. QC is work output, not workers, and therefore includes all work performed under this Task Order regardless of whether the work is performed by contractor personnel or by subcontractors. The contractor's QCP will set forth the staffing and procedures for self-inspecting the quality, timeliness, responsiveness, customer satisfaction, and other performance requirements in the PWS. The contractor will develop and implement a performance management system with processes to assess and report its performance to the designated government representative. The contractor's QCP will set forth the staffing and procedures for self-inspecting the quality, timeliness, responsiveness, customer satisfaction, and other performance requirements in the PWS. This QASP enables the government to take advantage of the contractor's QC program.

The government representative(s) will monitor performance and review performance reports furnished by the contractor to determine how the contractor is performing against communicated performance objectives. The government will make determination regarding incentives based on performance measurement metric data and notify the contractor of those decisions. The contractor will be responsible for making required changes in processes and practices to ensure performance is managed effectively.

2 ROLES AND RESPONSIBILITIES

2.1 The Contracting Officer

The contracting officer (CO) is responsible for monitoring contract compliance, contract administration, and cost control and for resolving any differences between the observations documented by contracting officer's representative (COR) and the contractor. The CO will designate one full-time COR, as the government authority for performance management. The number of additional representatives serving as technical inspectors depends on the complexity of the services measured, as well as the contractor's performance, and must be identified and designated by the CO.

2.2 The Contracting Officer's Representative

The contracting officer's representative (COR) is designated in writing by the CO to act as his or her authorized representative to assist in administering a contract. COR limitations are contained in the written appointment letter. The COR is responsible for technical administration of the project and ensures proper government surveillance of the contractor's performance. The COR is not empowered to make any contractual commitments or to authorize any contractual changes on the government's behalf. Any changes that the contractor deems may affect contract price, terms, or conditions shall be referred to the CO for action. The COTR will have the responsibility for completing QA monitoring forms used to document the inspection and

evaluation of the contractor's work performance. Government surveillance may occur under the inspection of services clause for any service relating to the contract.

2.3 The Assistant Contracting Officer's Representative

Due to the diversity of services on this Task Order, the Government shall assign multiple ACORs supporting the requirements of each major installation or program technical/functional area. The ACOR titles are identified below. ACORs monitor technical and functional aspects of the contract on a theater wide basis, as well as, administrative aspects of the contract on a regional basis. The ACORs are authorized to perform the following functions within their functional or technical area on behalf of the COR:

a. Assure that the Contractor performs the technical and administrative requirements of the contract
b. Perform inspections necessary in connection with Contractor performance
c. Maintain written and oral communications with The Contractor concerning technical aspects of the contract
d. Issue written interpretations of technical requirements, including Government drawings, designs, and specifications
e. Monitor Contractor's performance and notify both the COR and Contractor of any deficiencies

A letter of designation will be issued to each ACOR, a copy of which is sent to the Contractor, states the responsibilities and limitations of the respective ACOR, especially with regard to changes in cost or price, estimates or changes in delivery dates. ACORs are not authorized to change any of the terms and conditions of the resulting order.

2.4 The Assistant Contracting Officer's Representative by Technical or Functional Area

a. SCHQ IT Service Operations ACOR
b. JTF-Bravo IT Service Operations ACOR
c. JTF-GTMO IT Service Operations ACOR
d. SCO IT Service Operations ACOR
e. MNIS Service Operations ACOR
f. Enterprise Service Strategy, Design, and Transition ACOR
g. Continual Service Improvement ACOR
h. Enterprise Cyber Security Operations and Information Assurance ACOR
i. Enterprise Software Engineering and Integration/Application Development and Operations ACOR
j. Enterprise Unified Capabilities (Network Systems and Services) ACOR
k. Enterprise Data Center, Servers, and Storage ACOR
l. Enterprise Assistance and Advisory Services ACOR
m. Enterprise Cable Plant, LMR, Microwave and SATCOM ACOR
n. Enterprise Configuration Management ACOR
o. Enterprise Logistics Support ACOR

3 IDENTIFICATION OF REQUIRED PERFORMANCE STANDARDS/QUALITY LEVELS

The required performance standards and/or quality levels are included in the PWS and in Attachment 1, "Performance Requirements Summary." If the contractor meets the required service or performance level, it will be paid the monthly amount agreed on in the contract. Failure to meet the required service or performance level will result in a deduction from the monthly amount.

4 METHODOLOGIES TO MONITOR PERFORMANCE

4.1 Surveillance Techniques

In an effort to minimize the performance management burden, simplified surveillance methods shall be used by the government to evaluate contractor performance when appropriate. The primary methods of surveillance are (include those that apply)

Random monitoring, which shall be performed by the COR/ACOR designated inspector.

100% Inspection – Each month, the COR/ACOR, shall review the generated documentation and enter summary results into the Surveillance Activity Checklist.

Periodic Inspection – COR/ACOR typically performs the periodic inspection on a monthly basis.

4.2 Customer Feedback

The contractor is expected to establish and maintain professional communication between its personnel and customers. The primary objective of this communication is customer satisfaction. Customer satisfaction is the most significant external indicator of the success and effectiveness of all services provided and can be measured through customer complaints.

Performance management drives the contractor to be customer focused through initially and internally addressing customer complaints and investigating the issues and/or problems. The customer always has the option to communicate complaints to the COR or ACOR, as opposed to the contractor.

Customer complaints, to be considered valid, must set forth clearly and in writing the detailed nature of the complaint, must be signed, and must be forwarded to the COTR/COR. The COTR/COR will accept those customer complaints and investigate using the Quality Assurance Monitoring Form – Customer Complaint Investigation, identified in Appendix 3.

Customer feedback may also be obtained either from the results of formal customer satisfaction surveys or from random customer complaints.

4.3 Acceptable Performance Levels

The acceptable performance levels included in Appendix 1, Performance Requirements Summary Table, for contractor performance are structured to allow the contractor to manage how the work is performed while providing negative incentives for performance shortfalls.

5. QUALITY ASSURANCE DOCUMENTATION

5.1 The Performance Management Feedback Loop

The performance management feedback loop begins with the communication of expected outcomes. Performance standards are expressed in the PWS and are assessed using the performance monitoring techniques shown in Attachment 1.

5.2 Monitoring Forms

The government's QA surveillance, accomplished by the COR/ACOR, will be reported using the monitoring forms in Attachments 2 and 3. The forms, when completed, will document the government's assessment of the contractor's performance under the contract to ensure that the required service levels are being achieved.

The COR will retain a copy of all completed QA surveillance forms.

6 ANALYSIS OF QUALITY ASSURANCE ASSESSMENT

6.1 Determining Performance

Government shall use the monitoring methods cited to determine whether the performance standards/service levels/AQLs have been met. If the contractor has not met the minimum requirements, it may be asked to develop a corrective action plan to show how and by what date it intends to bring performance up to the required levels.

6.2 Reporting

At the end of each month, the COR will prepare a written report for the ACO summarizing the overall results of the quality assurance surveillance of the contractor's performance. This written report, which includes the contractor's submitted monthly report and the completed quality assurance monitoring forms (Attachment 2), will become part of the QA documentation. It will enable the government to demonstrate whether the contractor is meeting the stated objectives and/or performance standards, including cost/technical/scheduling objectives.

6.3 Reviews and Resolution

The COR required the contractor's project manager, or a designated alternate, to meet with the COR or ACOR and other government personnel as deemed necessary to discuss performance evaluation. The COR will define a frequency of in-depth reviews with the contractor, including appropriate self-assessments by the contractor; however, if the need arises, the contractor will meet with the COR or appropriate ACOR as often as required or per the contractor's request. The agenda of the reviews may include:

a. Monthly performance assessment data and trend analysis
b. Issues and concerns of both parties
c. Projected outlook for upcoming months and progress against expected trends, including a corrective action plan analysis
d. Recommendations for improved efficiency and/or effectiveness
e. Issues arising from KPI or Minimum Performance Requirements reporting

The COR must coordinate and communicate with the Contractor to resolve issues and concerns regarding marginal or unacceptable performance.

The COR and the Contractor should jointly formulate tactical and long-term courses of action. Decisions regarding changes to metrics, thresholds, or service levels should be clearly documented. Changes to service levels, procedures, and metrics will be incorporated as a contract modification at the convenience of the PCO/ACO.

APPENDIX 1: PERFORMANCE REQUIREMENTS SUMMARY

The Contractor Performance requirements are summarized into performance objectives that relate directly to mission essential items. The performance threshold briefly describes the minimum acceptable levels of service required for each requirement. These thresholds are critical to mission success. Task Order surveillance will be performed by the COR and appropriate ACORS.

Performance Objectives	Performance Standards	Performance Threshold	Methods of Surveillance	Impact on Contractor Payments or Other Impact
PRS #1 Accomplishment of Planning, Designing, Phase – In of work responsibilities or Transition New Technical/Operational Capabilities References: IT Service Strategy, (PWS 5.1.1) IT Service Design (PWS 5.1.2) IT Service Transition (PWS 5.1.3)	Technical performance. Meet the approved technical requirements, technical design and technical performance. Schedule. Meet the approved capability delivery schedules (Applies to JIE or New Capability CLINs) Timeliness of deliverables. Provide required documentation and reports in accordance with schedules. Resource control and Management. Meet milestones or complete deliveries within approved labor hours and labor costs. (Time and Materials CLINs Only)	For New/Modified Capabilities, Passes Acceptance Testing and conforms to Functional and Physical Configuration Audits. Within +/- 15% of the agreed schedule Within +/- 15% of the agreed schedule Within +/- 10% of agreed resources (labor hours or labor costs for Time and Material	100% Review of Deliverables	Positive Comments and Ratings or Negative comment and ratings respectively for successful or unsuccessful performance. Possible exercise of options for successful performance. Possible decision to not exercise future options for unsuccessful performance.

		CLINs)		
PRS #2 Meet Performance Requirements for All Services References IT Service Operations (PWS 5.1.4)	Meet performance requirements for all services identified in attachment 9 Timeliness of deliverables. Provide required documentation and reports in accordance with schedules.	Availability in accordance with attachment 9 Within +/- 15% of the agreed schedule	100% Review of Deliverables	Positive Comments and Ratings or Negative comment and ratings respectively for successful or unsuccessful performance. Possible exercise of options for successful performance. Possible decision to not exercise future options for unsuccessful performance.

PRS #3 Ability to Identify Process Improvements or Efficiencies Reference: Continuous IT Service Improvement (PWS 5.1.7)	Timeliness of deliverables. Provide required documentation and reports in accordance with schedules.	Within +/- 15% of the agreed schedule	100% Review of Deliverables	Positive Comments and Ratings or Negative comment and ratings respectively for successful or unsuccessful performance. Possible exercise of options for successful performance. Possible decision to not exercise future options for unsuccessful performance.
PRS #4 Accomplish Software Engineering and Integration Activities Reference Software Engineering Integration Life Cycle Support Activities (PWS 5.1.9)	Technical performance. Meet the approved technical requirements, technical design and technical performance. Schedule. Meet the approved capability delivery schedules (Applies to JIE or New Capability CLINs) Timeliness of deliverables. Provide required documentation and reports in accordance with schedules. Resource control and Management. Meet milestones or complete deliveries within approved	For SEI Capabilities, Passes Acceptance Testing and conforms to Functional and Physical Configuration Audits. Within +/- 15% of the agreed schedule Within +/- 15% of the agreed schedule Within +/- 10% of	100% Review of Deliverables	Positive Comments and Ratings or Negative comment and ratings respectively for successful or unsuccessful performance. Possible exercise of options for successful performance. Possible decision to not exercise future options for unsuccessful performance.

	labor hours and labor costs. (Time and Materials CLINs Only)	agreed resources (labor hours or labor costs for Time and Material CLINs)		
PRS #5 Accomplish IT Systems Support Services Reference: IT Systems Support Services (PWS 5.1.10)	Timeliness of deliverables. Provide required documentation and reports in accordance with schedules.	Within +/- 15% of the agreed schedule	100% Review of Deliverables	Positive Comments and Ratings or Negative comment and ratings respectively for successful or unsuccessful performance. Possible exercise of options for successful performance. Possible decision to not exercise future options for unsuccessful performance.
PRS #6 Accomplish Other Required Support Services in Colombia, JTF-Bravo, and JTF-GTMO Reference: Other Required Support Colombia, (JTF-Bravo, JTF-GTMO) (PWS 5.1.11)	Timeliness of deliverables. Provide required documentation and reports in accordance with schedules.	Within +/- 15% of the agreed schedule	100% Review of Deliverables	Positive Comments and Ratings or Negative comment and ratings respectively for successful or unsuccessful performance. Possible exercise of options for successful performance. Possible decision to not exercise future options for unsuccessful performance.

PRS #7 Accomplish Exercise and Contingency Operations Support Reference: Exercise and Contingency Operations Support PWS Paragraph 5.2.5	Timeliness of deliverables. Provide required documentation and reports in accordance with schedules.	Within +/- 15% of the agreed schedule	100% Review of Deliverables	Positive Comments and Ratings or Negative comment and ratings respectively for successful or unsuccessful performance. Possible exercise of options for successful performance. Possible decision to not exercise future options for unsuccessful performance.

ATTACHMENT 7 - APPENDIX 2: SAMPLE QUALITY ASSURANCE MONITORING FORM

SERVICE or STANDARD: _____

_____

_____

_____

_____

SURVEY PERIOD: _____

SURVEILLANCE METHOD (Check):

❒ Random Sampling ❒ 100% Inspection ❒ Periodic Inspection ❒ Customer Complaint

LEVEL OF SURVEILLANCE (Check):

❒ Monthly ❒ Quarterly ❒ As needed

PERCENTAGE OF ITEMS SAMPLED DURING SURVEY PERIOD: _____ %

ANALYSIS OF RESULTS:

Observed Service Provider Performance Measurement Rate: _____%

Service Provider's Performance (Check): ❒ Meets Standards

❒ Does Not Meet Standards

Narrative of Performance During Survey Period: _____

_____

_____

_____

_____

PREPARED BY: _____ **DATE:** _____

ATTACHMENT 7 - APPENDIX 3 CUSTOMER COMPLAINT INVESTIGATON FORM

TO BE DEVELOPED JOINTLY BY AWARDEE AND GOVERNMENT AFTER CONTRACT AWARD

QUALITY ASSURANCE SURVEILLANCE PLAN (QASP)

1. INTRODUCTION

This quality assurance surveillance plan (QASP) is pursuant to the requirements listed in the performance work statement (PWS) entitled U.S. SOUTHERN COMMAND (USSOUTHCOM) ENTERPRISE INFORMATION TECHNOLOGY SERVICES SUPPORT CONTRACT (EITSSC). This plan sets forth the procedures and guidelines USSOUTHCOM J6 will use in ensuring the required performance standards or services levels are achieved by the contractor.

1.1 Purpose

The purpose of the QASP is to describe the systematic methods used to monitor performance and to identify the required documentation and the resources to be employed. The QASP provides a means for evaluating whether the contractor is meeting the performance standards/quality levels identified in the PWS and the contractor's quality control plan (QCP), and to ensure that the government pays only for the level of services received.

This QASP defines the roles and responsibilities of all members of the integrated project team (IPT), identifies the performance objectives, defines the methodologies used to monitor and evaluate the contractor's performance, describes quality assurance documentation requirements, and describes the analysis of quality assurance monitoring results.

1.2 Performance Management Approach

The PWS structures the acquisition around "what" service or quality level is required, as opposed to "how" the contractor should perform the work (i.e., results, not compliance). This QASP will define the performance management approach taken by USSOUTHCOM J6 to monitor and manage the contractor's performance to ensure the expected outcomes or performance objectives communicated in the PWS are achieved. Performance management rests on developing a capability to review and analyze information generated through performance assessment. The ability to make decisions based on the analysis of performance data is the cornerstone of performance management; this analysis yields information that indicates whether expected outcomes for the project are being achieved by the contractor.

Performance management represents a significant shift from the more traditional quality assurance (QA) concepts in several ways. Performance management focuses on assessing whether outcomes are being achieved and to what extent. This approach migrates away from scrutiny of compliance with the processes and practices used to achieve the outcome. A performance-based approach enables the contractor to play a large role in how the work is performed, as long as the proposed processes are within the stated constraints. The only exceptions to process reviews are those required by law (federal, state, and local) and compelling business situations, such as safety and health. A "results" focus provides the contractor flexibility to continuously improve and innovate over the course of the contract as

long as the critical outcomes expected are being achieved and/or the desired performance levels are being met.

1.3 Performance Management Strategy

The contractor is responsible for the quality of all work performed. The contractor measures that quality through the contractor's own quality control (QC) program. QC is work output, not workers, and therefore includes all work performed under this Task Order regardless of whether the work is performed by contractor personnel or by subcontractors. The contractor's QCP will set forth the staffing and procedures for self-inspecting the quality, timeliness, responsiveness, customer satisfaction, and other performance requirements in the PWS. The contractor will develop and implement a performance management system with processes to assess and report its performance to the designated government representative. The contractor's QCP will set forth the staffing and procedures for self-inspecting the quality, timeliness, responsiveness, customer satisfaction, and other performance requirements in the PWS. This QASP enables the government to take advantage of the contractor's QC program.

The government representative(s) will monitor performance and review performance reports furnished by the contractor to determine how the contractor is performing against communicated performance objectives. The government will make determination regarding incentives based on performance measurement metric data and notify the contractor of those decisions. The contractor will be responsible for making required changes in processes and practices to ensure performance is managed effectively.

2 ROLES AND RESPONSIBILITIES

2.1 The Contracting Officer

The contracting officer (CO) is responsible for monitoring contract compliance, contract administration, and cost control and for resolving any differences between the observations documented by contracting officer's representative (COR) and the contractor. The CO will designate one full-time COR, as the government authority for performance management. The number of additional representatives serving as technical inspectors depends on the complexity of the services measured, as well as the contractor's performance, and must be identified and designated by the CO.

2.2 The Contracting Officer's Representative

The contracting officer's representative (COR) is designated in writing by the CO to act as his or her authorized representative to assist in administering a contract. COR limitations are contained in the written appointment letter. The COR is responsible for technical administration of the project and ensures proper government surveillance of the contractor's performance. The COR is not empowered to make any contractual commitments or to authorize any contractual changes on the government's behalf. Any changes that the contractor deems may affect contract price, terms, or conditions shall be referred to the CO for action. The COTR will have the responsibility for completing QA monitoring forms used to document the inspection and

evaluation of the contractor's work performance. Government surveillance may occur under the inspection of services clause for any service relating to the contract.

2.3 The Assistant Contracting Officer's Representative

Due to the diversity of services on this Task Order, the Government shall assign multiple ACORs supporting the requirements of each major installation or program technical/functional area. The ACOR titles are identified below. ACORs monitor technical and functional aspects of the contract on a theater wide basis, as well as, administrative aspects of the contract on a regional basis. The ACORs are authorized to perform the following functions within their functional or technical area on behalf of the COR:

a. Assure that the Contractor performs the technical and administrative requirements of the contract
b. Perform inspections necessary in connection with Contractor performance
c. Maintain written and oral communications with The Contractor concerning technical aspects of the contract
d. Issue written interpretations of technical requirements, including Government drawings, designs, and specifications
e. Monitor Contractor's performance and notify both the COR and Contractor of any deficiencies

A letter of designation will be issued to each ACOR, a copy of which is sent to the Contractor, states the responsibilities and limitations of the respective ACOR, especially with regard to changes in cost or price, estimates or changes in delivery dates. ACORs are not authorized to change any of the terms and conditions of the resulting order.

2.4 The Assistant Contracting Officer's Representative by Technical or Functional Area

a. SCHQ IT Service Operations ACOR
b. JTF-Bravo IT Service Operations ACOR
c. JTF-GTMO IT Service Operations ACOR
d. SCO IT Service Operations ACOR
e. MNIS Service Operations ACOR
f. Enterprise Service Strategy, Design, and Transition ACOR
g. Continual Service Improvement ACOR
h. Enterprise Cyber Security Operations and Information Assurance ACOR
i. Enterprise Software Engineering and Integration/Application Development and Operations ACOR
j. Enterprise Unified Capabilities (Network Systems and Services) ACOR
k. Enterprise Data Center, Servers, and Storage ACOR
l. Enterprise Assistance and Advisory Services ACOR
m. Enterprise Cable Plant, LMR, Microwave and SATCOM ACOR
n. Enterprise Configuration Management ACOR
o. Enterprise Logistics Support ACOR

3 IDENTIFICATION OF REQUIRED PERFORMANCE STANDARDS/QUALITY LEVELS

The required performance standards and/or quality levels are included in the PWS and in Attachment 1, "Performance Requirements Summary." If the contractor meets the required service or performance level, it will be paid the monthly amount agreed on in the contract. Failure to meet the required service or performance level will result in a deduction from the monthly amount.

4 METHODOLOGIES TO MONITOR PERFORMANCE

4.1 Surveillance Techniques

In an effort to minimize the performance management burden, simplified surveillance methods shall be used by the government to evaluate contractor performance when appropriate. The primary methods of surveillance are (include those that apply)

Random monitoring, which shall be performed by the COR/ACOR designated inspector.

100% Inspection – Each month, the COR/ACOR, shall review the generated documentation and enter summary results into the Surveillance Activity Checklist.

Periodic Inspection – COR/ACOR typically performs the periodic inspection on a monthly basis.

4.2 Customer Feedback

The contractor is expected to establish and maintain professional communication between its personnel and customers. The primary objective of this communication is customer satisfaction. Customer satisfaction is the most significant external indicator of the success and effectiveness of all services provided and can be measured through customer complaints.

Performance management drives the contractor to be customer focused through initially and internally addressing customer complaints and investigating the issues and/or problems. The customer always has the option to communicate complaints to the COR or ACOR, as opposed to the contractor.

Customer complaints, to be considered valid, must set forth clearly and in writing the detailed nature of the complaint, must be signed, and must be forwarded to the COTR/COR. The COTR/COR will accept those customer complaints and investigate using the Quality Assurance Monitoring Form – Customer Complaint Investigation, identified in Appendix 3.

Customer feedback may also be obtained either from the results of formal customer satisfaction surveys or from random customer complaints.

4.3 Acceptable Performance Levels

The acceptable performance levels included in Appendix 1, Performance Requirements Summary Table, for contractor performance are structured to allow the contractor to manage how the work is performed while providing negative incentives for performance shortfalls.

5. QUALITY ASSURANCE DOCUMENTATION

5.1 The Performance Management Feedback Loop

The performance management feedback loop begins with the communication of expected outcomes. Performance standards are expressed in the PWS and are assessed using the performance monitoring techniques shown in Attachment 1.

5.2 Monitoring Forms

The government's QA surveillance, accomplished by the COR/ACOR, will be reported using the monitoring forms in Attachments 2 and 3. The forms, when completed, will document the government's assessment of the contractor's performance under the contract to ensure that the required service levels are being achieved.

The COR will retain a copy of all completed QA surveillance forms.

6 ANALYSIS OF QUALITY ASSURANCE ASSESSMENT

6.1 Determining Performance

Government shall use the monitoring methods cited to determine whether the performance standards/service levels/AQLs have been met. If the contractor has not met the minimum requirements, it may be asked to develop a corrective action plan to show how and by what date it intends to bring performance up to the required levels.

6.2 Reporting

At the end of each month, the COR will prepare a written report for the ACO summarizing the overall results of the quality assurance surveillance of the contractor's performance. This written report, which includes the contractor's submitted monthly report and the completed quality assurance monitoring forms (Attachment 2), will become part of the QA documentation. It will enable the government to demonstrate whether the contractor is meeting the stated objectives and/or performance standards, including cost/technical/scheduling objectives.

6.3 Reviews and Resolution

The COR required the contractor's project manager, or a designated alternate, to meet with the COR or ACOR and other government personnel as deemed necessary to discuss performance evaluation. The COR will define a frequency of in-depth reviews with the contractor, including appropriate self-assessments by the contractor; however, if the need arises, the contractor will meet with the COR or appropriate ACOR as often as required or per the contractor's request. The agenda of the reviews may include:

a. Monthly performance assessment data and trend analysis
b. Issues and concerns of both parties
c. Projected outlook for upcoming months and progress against expected trends, including a corrective action plan analysis
d. Recommendations for improved efficiency and/or effectiveness
e. Issues arising from KPI or Minimum Performance Requirements reporting

The COR must coordinate and communicate with the Contractor to resolve issues and concerns regarding marginal or unacceptable performance.

The COR and the Contractor should jointly formulate tactical and long-term courses of action. Decisions regarding changes to metrics, thresholds, or service levels should be clearly documented. Changes to service levels, procedures, and metrics will be incorporated as a contract modification at the convenience of the PCO/ACO.

APPENDIX 1: PERFORMANCE REQUIREMENTS SUMMARY

The Contractor Performance requirements are summarized into performance objectives that relate directly to mission essential items. The performance threshold briefly describes the minimum acceptable levels of service required for each requirement. These thresholds are critical to mission success. Task Order surveillance will be performed by the COR and appropriate ACORS.

Performance Objectives	Performance Standards	Performance Threshold	Methods of Surveillance	Impact on Contractor Payments or Other Impact
PRS #1 Accomplishment of Planning, Designing, Phase – In of work responsibilities or Transition New Technical/Operational Capabilities References: IT Service Strategy, (PWS 5.1.1) IT Service Design (PWS 5.1.2) IT Service Transition (PWS 5.1.3)	Technical performance. Meet the approved technical requirements, technical design and technical performance. Schedule. Meet the approved capability delivery schedules (Applies to JIE or New Capability CLINs) Timeliness of deliverables. Provide required documentation and reports in accordance with schedules. Resource control and Management. Meet milestones or complete deliveries within approved labor hours and labor costs. (Time and Materials CLINs Only)	For New/Modified Capabilities, Passes Acceptance Testing and conforms to Functional and Physical Configuration Audits. Within +/- 15% of the agreed schedule Within +/- 15% of the agreed schedule Within +/- 10% of agreed resources (labor hours or labor costs for Time and Material	100% Review of Deliverables	Positive Comments and Ratings or Negative comment and ratings respectively for successful or unsuccessful performance. Possible exercise of options for successful performance. Possible decision to not exercise future options for unsuccessful performance.

		CLINs)		
PRS #2 Meet Performance Requirements for All Services References IT Service Operations (PWS 5.1.4)	Meet performance requirements for all services identified in attachment 9 Timeliness of deliverables. Provide required documentation and reports in accordance with schedules.	Availability in accordance with attachment 9 Within +/- 15% of the agreed schedule	100% Review of Deliverables	Positive Comments and Ratings or Negative comment and ratings respectively for successful or unsuccessful performance. Possible exercise of options for successful performance. Possible decision to not exercise future options for unsuccessful performance.

PRS #3 Ability to Identify Process Improvements or Efficiencies Reference: Continuous IT Service Improvement (PWS 5.1.7)	Timeliness of deliverables. Provide required documentation and reports in accordance with schedules.	Within +/- 15% of the agreed schedule	100% Review of Deliverables	Positive Comments and Ratings or Negative comment and ratings respectively for successful or unsuccessful performance. Possible exercise of options for successful performance. Possible decision to not exercise future options for unsuccessful performance.
PRS #4 Accomplish Software Engineering and Integration Activities Reference Software Engineering Integration Life Cycle Support Activities (PWS 5.1.9)	Technical performance. Meet the approved technical requirements, technical design and technical performance. Schedule. Meet the approved capability delivery schedules (Applies to JIE or New Capability CLINs) Timeliness of deliverables. Provide required documentation and reports in accordance with schedules. Resource control and Management. Meet milestones or complete deliveries within approved	For SEI Capabilities, Passes Acceptance Testing and conforms to Functional and Physical Configuration Audits. Within +/- 15% of the agreed schedule Within +/- 15% of the agreed schedule Within +/- 10% of	100% Review of Deliverables	Positive Comments and Ratings or Negative comment and ratings respectively for successful or unsuccessful performance. Possible exercise of options for successful performance. Possible decision to not exercise future options for unsuccessful performance.

	labor hours and labor costs. (Time and Materials CLINs Only)	agreed resources (labor hours or labor costs for Time and Material CLINs)		
PRS #5 Accomplish IT Systems Support Services Reference: IT Systems Support Services (PWS 5.1.10)	Timeliness of deliverables. Provide required documentation and reports in accordance with schedules.	Within +/- 15% of the agreed schedule	100% Review of Deliverables	Positive Comments and Ratings or Negative comment and ratings respectively for successful or unsuccessful performance. Possible exercise of options for successful performance. Possible decision to not exercise future options for unsuccessful performance.
PRS #6 Accomplish Other Required Support Services in Colombia, JTF-Bravo, and JTF-GTMO Reference: Other Required Support Colombia, (JTF-Bravo, JTF-GTMO) (PWS 5.1.11)	Timeliness of deliverables. Provide required documentation and reports in accordance with schedules.	Within +/- 15% of the agreed schedule	100% Review of Deliverables	Positive Comments and Ratings or Negative comment and ratings respectively for successful or unsuccessful performance. Possible exercise of options for successful performance. Possible decision to not exercise future options for unsuccessful performance.

PRS #7 Accomplish Exercise and Contingency Operations Support Reference: Exercise and Contingency Operations Support PWS Paragraph 5.2.5	Timeliness of deliverables. Provide required documentation and reports in accordance with schedules.	Within +/- 15% of the agreed schedule	100% Review of Deliverables	Positive Comments and Ratings or Negative comment and ratings respectively for successful or unsuccessful performance. Possible exercise of options for successful performance. Possible decision to not exercise future options for unsuccessful performance.

ATTACHMENT 7 - APPENDIX 2: SAMPLE QUALITY ASSURANCE MONITORING FORM

SERVICE or STANDARD: _____

_____

_____

_____

_____

SURVEY PERIOD: _____

SURVEILLANCE METHOD (Check):

☐ Random Sampling ☐ 100% Inspection ☐ Periodic Inspection ☐ Customer Complaint

LEVEL OF SURVEILLANCE (Check):

☐ Monthly ☐ Quarterly ☐ As needed

PERCENTAGE OF ITEMS SAMPLED DURING SURVEY PERIOD: _____ %

ANALYSIS OF RESULTS:

Observed Service Provider Performance Measurement Rate: _____%

Service Provider's Performance (Check): ☐ Meets Standards

☐ Does Not Meet Standards

Narrative of Performance During Survey Period: _____

_____

_____

_____

_____

PREPARED BY: _____ **DATE:** _____

ATTACHMENT 7 - APPENDIX 3 CUSTOMER COMPLAINT INVESTIGATON FORM

TO BE DEVELOPED JOINTLY BY AWARDEE AND GOVERNMENT AFTER CONTRACT AWARD