

Performance Work Statement

For Cybersecurity Support

of Offutt AFB

55th Strategic Communications Squadron (55 SCS)

Defense Red Switch Network and other

Nuclear Command, Control, and Communications

(NC3) Missions

## TABLE OF CONTENTS

SECTION	PARAGRAPH/TITLE	PAGE
1.	SECTION 1 – SUPPORT OVERVIEW.....	4
1.1.	BACKGROUND.....	4
1.2.	OBJECTIVES.....	5
1.3.	GENERAL CONTRACTOR REQUIREMENTS	
1.3.1.	PERSONNEL MANAGEMENT.....	5
1.3.1.1.	POINTS OF CONTACT.....	6
1.3.1.2.	CONTRACTOR PROGRAM MANAGEMENT.....	6
1.3.2.	TRAINING.....	6
1.3.2.1.	OTHER GOVERNMENT-PROVIDED TRAINING.....	7
1.3.2.1.1.	SECURITY TRAINING.....	7
1.3.2.1.2.	NETWORK USER TRAINING.....	7
1.3.2.1.3.	MISSION-FOCUSED TRAINING.....	7
1.3.2.2.	EDUCATION, CERTIFICATIONS, & WORK EXPERIENCE.....	7
1.3.2.3.	TRAINING RECORDS.....	8
1.3.3.	SECURITY.....	8
1.3.3.1.	INSTALLATION ACCESS AND PHYSICAL SECURITY.....	8
1.3.3.2.	FACILITY SECURITY CLEARANCE (FCL).....	8
1.3.3.3.	PERSONNEL SECURITY CLEARANCE.....	8
1.3.3.4.	FACILITY ACCESS.....	9
1.3.3.5.	CONTRACTOR ACCESS.....	9
1.3.3.6.	PRIVACY ACT.....	9
1.3.3.7.	NO RIGHT TO PRIVACY.....	10
1.3.3.8.	INFORMATION SECURITY (INFOSEC).....	10
1.3.3.9.	SECURITY MANAGEMENT (TRANSMISSION OF CLASSIFIED MATERIAL).....	10
1.3.3.10.	CLASSIFIED DESTRUCTION.....	10
1.3.4.	QUALITY ASSURANCE MANAGEMENT.....	10
1.3.4.1.	PERFORMANCE MEETINGS.....	11
1.3.4.2.	GOVERNMENT QUALITY ASSURANCE SURVEILLANCE PROGRAM.....	11
1.3.5.	APPEARANCE AND STANDARDS OF CONDUCT.....	11
1.3.6.	CONTINUATION OF DoW CONTRACTOR SERVICES DURING CRISES.....	12
1.3.7.	GOVERNMENT SITE RULES.....	12
1.3.8.	PERIOD OF PERFORMANCE.....	13
2.	SECTION 2 – CONTRACTOR CYBERSECURITY SUPPORT REQUIREMENTS .....	13
2.1.	<b>CLIN 001 - DRSN CYBERSECURITY SUPPORT.....</b>	13
2.2.	<b>CLIN 002- GLOBAL AIRCREW STRATEGIC NETWORK TERMINAL (G-ASNT)</b> CYBERSECURITY SUPPORT.....	16
2.3.	<b>CLIN 003 - NON-HARDENED AIRCREW ALERTING SYSTEM (NAAS) – KLAXON</b> CYBERSECURITY SUPPORT.....	17
2.4.	<b>CLIN 004 - OTHER 55 SCS CYBERSECURITY SUPPORT.....</b>	18
2.4.1.	OTHER TERMS OF SUPPORT.....	18
2.5.	<b>CLIN 005 - TDY/TRAVEL.....</b>	19

3. SECTION 3 – GOVERNMENT-FURNISHED PROPERTY AND SERVICES.....	19
3.1. GOVERNMENT FACILITIES.....	19
3.2. GOVERNMENT PROPERTY.....	19
3.3. CONTRACTOR PROPERTY MANAGEMENT.....	20
3.4. UTILITIES.....	20
3.5. INSTALLATION MAIL DISTRIBUTION.....	20
3.6. TELEPHONE.....	20
3.7. COMPUTER.....	20
3.8. FORMS AND PUBLICATIONS.....	20
3.9. REFUSE COLLECTION.....	20
3.10. INSECTS AND RODENT CONTROL.....	20
3.11. SECURITY POLICE.....	21
3.12. BASE CIVIL ENGINEERING.....	21
3.13. EMERGENCY MEDICAL SERVICES.....	21
3.14. TRANSPORTATION.....	21
4. SECTION 4 – TECHNICAL DEFINITIONS.....	22
4.1. TECHNICAL TERMINOLOGY.....	22
4.2. ACRONYMS.....	24
4.3. REFERENCE DOCUMENTS.....	27

## **1. SUPPORT OVERVIEW**

### **1.1. BACKGROUND**

The 55th Strategic Communications Squadron (55 SCS) operates and maintains numerous nuclear command, control, and communications (NC3) systems.

The Defense Red Switch Network (DRSN) Command and Control Switching System (CCSS) provides mission-essential, critical secure and non-secure voice services to the National Command Authority (NCA), the Department of War (DoW), various federal agencies, and Foreign Allies. The Red and Black DRSN Switches (six DSS-2As) supporting the United States Strategic Command (USSTRATCOM) Global Operations Center (GOC) provide the ability to convene and manage our nation's most critical national-level secure and non-secure voice conferencing requirements. These conferences support the entire spectrum of USSTRATCOM mission assignments and may be assembled at any time to support the nation's senior leaders during times of national emergencies and crises involving USSTRATCOM and other DoW assets worldwide.

DRSN, an element of the Defense Information Systems Network (DISN), is a network of secure command and control switches that provide high-quality secure voice and conferencing capabilities to senior decision makers and staff of the Military Departments (MILDEPs), the Combatant Commanders (COCOMs), Major Commands (MAJCOMs), other Government departments and agencies, and U.S. Allies.

The mission of DRSN is to provide the ability to transfer voice and data between the MILDEPs, the National Military Command Center (NMCC), combatant commands, military services, subordinate organizations (military and civilian), and Allies (North Atlantic Treaty Organization (NATO), Canada, etc.), both locally and worldwide. DRSN also provides secure voice conferencing and gateway access to secure strategic, tactical, airborne, and seaborne equipment and platforms.

DRSN consists of four major subsystems: (1) Switching Subsystem, (2) Transmission Subsystem, (3) Timing and Synchronization (T&S) Subsystem, and (4) Network Management Subsystem (NMS). Cybersecurity support for all subsystems and related components is required for establishing and maintaining a full DRSN Authorization to Operate (ATO).

The Global Aircrew Strategic Network Terminal (G-ASNT) is an Air Force Global Strike Command (AFGSC) nuclear command, control and communications system utilizing a satellite constellation to link national command authorities to warfighters via a protected, robust communication system, to missile, nuclear bomber, and support aircraft crews in austere operational environments. Offutt AFB has a fixed G-ASNT terminal in the 55 Wing Command Post, and three transportable G-ASNT terminals in the 55 SCS. G-ASNT is being fielded in increments. Increment one supports the satellite communication requirement. Increment two, block one supports EMP-hardened aircrew alerting (used to support USSTRATCOM's Looking Glass mission) and UHF radios. Increment three will provide HF capabilities once it is designed and fielded.

The Non-hardened Aircrew Alerting System (NAAS) Klaxon is a NC3 terrestrial-based aircrew alerting system that supports the National Airborne Operations Center (NAOC) aircrew alerting requirements. It is

a Windows OS-based system that operates as a stand-alone network. It has four servers, which are used individually for activating or testing the klaxon lights and sounders.

## **1.2. OBJECTIVES**

The objective of this Performance Work Statement (PWS) is to identify requirements to provide the Government with high-quality, cost-effective, dedicated cybersecurity support to the 55 SCS for its DRSN and NC3 systems. The goal is to ensure Risk Management Framework (RMF) requirements are met, Authority to Operate (ATO) is granted and remains valid, all security-related documentation is kept up-to-date, and supported units have a team of cybersecurity experts on which to rely. To successfully fulfill this requirement, a combination of Cybersecurity Specialist and Information Systems Security Officer (ISSO) support will be provided to address tasks outlined in this PWS for named NC3 systems. ISSO support is also solicited to maintain Offutt DRSN accreditation associated with segments of multiple NC3 systems that connect to Offutt DRSN, such as the Survivable Emergency Conferencing Network Digitization (SECN-DZ), Presidential and National Voice Conferencing (PNVC), and various gateways and long local communications circuits. Additionally, personnel shall be required to assist in configuration management process reviews to ensure appropriate mechanisms are in place, update DRSN RMF Body of Evidence requirements, and support DRSN external entity audits and inspections.

## **1.3. GENERAL CONTRACTOR REQUIREMENTS**

This PWS outlines general requirements for contractor performance in the areas outlined below:

- a. Personnel Management
- b. Training
- c. Security
- d. Quality Assurance Management
- e. Standards of Conduct and Appearance
- f. Continuation of Essential DoW Contractor Services During Crises
- g. Government Site Rules

### **1.3.1. PERSONNEL MANAGEMENT**

The contractor shall maintain appropriately-skilled and credentialed cybersecurity personnel and supervisory functions to deliver cybersecurity services, as defined in this PWS. The contractor shall be responsible for personnel selection, supervision, and assignment. The contractor's on-site personnel shall be easily distinguishable as contractor representatives (e.g. badge, hat, or lanyard). The primary places of performance are, but not limited to, USSTRATCOM, Buildings 1000 and 1022, Rooms NL1.100A, NL1.100B, MSDC-2 (SL2.148), MSDC-4 (SL2.140), ITER A (HL2.128), ITER B (HL2.126), and various telecommunications closets located on Offutt AFB, Nebraska. Daytime support is required Monday through Friday, with occasional weekend support under extenuating circumstances. Any scheduled and unscheduled employee absences shall be coordinated by contractor management to ensure continuity of operations with no mission degradation. Upon the retirement, resignation, reassignment, or dismissal of an employee, the contractor shall fill any vacancies with fully-qualified personnel within thirty (30) calendar days of release.

### **1.3.1.1. POINTS OF CONTACT (POC)**

The contractor shall designate primary and alternate focal points via written correspondence to the Procurement Contracting Officer (PCO) at Offutt AFB, Nebraska within thirty (30) calendar days post-contract award. The primary and alternate POCs shall be responsible for managing cybersecurity services for the 55 SCS. At least one shall be reachable twenty-four (24) hours per day, seven (7) days per week (including Federal Holidays). POC changes shall be provided to the PCO within two (2) calendar days of changes.

### **1.3.1.2. CONTRACTOR PROGRAM MANAGEMENT**

Contractor employees shall possess all current training, qualifications, and experience necessary to accomplish the requirements of this PWS. A designated contractor Program Manager (PM) shall oversee contractor/subcontractor employees, be responsible for task direction, and interface with the Contracting Officer (CO), Contracting Officer Representative (COR), Offutt Red Switch Management Office (ORSMO), and 55 SCS leadership. The contractor shall be responsible for providing and retaining a well-qualified, professional, motivated work force, and for fostering a culture that emphasizes teamwork, integrity, continuous improvement, and effective resource management. The contractor shall integrate and coordinate all activities necessary to successfully execute these requirements within normally-scheduled hours.

### **1.3.2. TRAINING**

All personnel permanently-assigned, or who will provide backfill support to designated Government sites, must be fully-trained and qualified to oversee all ATO aspects of the complement of NC3-related equipment and services at Offutt AFB, Nebraska. The contractor shall develop a training plan that will ensure contractor personnel are adequately trained to meet the requirements of this PWS, and submit the plan to the PCO for review/approval not later than thirty (30) calendar days after contract award. The contractor shall have a working knowledge of Emissions Security (EMSEC) and Telecommunications Electronics Material Protected from Emanating Spurious Transmissions (TEMPEST) concepts. On-the-job training may be accomplished using existing facilities, but only on a non-interference basis, such that system operation and operational missions are not adversely impacted. The contractor shall be authorized to send ISSOs to initial or refresher DSS-2A Switch training at the CCSS training school located at Ft Huachuca, AZ, but is responsible for all travel costs. To schedule training at the CCSS training school, the contractor must coordinate training requirements with ORSMO. The Government shall only provide additional DSS-2A training to ISSOs for significant changes to CCSS equipment, or supplementary subsystems, required for sustainment of the ATO. The contractor shall also be authorized to send ISSOs to other Government-sponsored training, such as Global Aircrew Strategic Network Terminal (G-ASNT) operator and maintenance courses, as well as Enterprise Mission Assurance Support Service (eMASS) workflow platform training, etc., as required to support RMF package development. Again, the

contractor shall be responsible for any travel expenses. Contractor employees who attend the CCSS training school, and other Government training courses, shall provide copies of their certifications to the COR/PCO within thirty (30) days of completion.

### **1.3.2.1 OTHER GOVERNMENT-PROVIDED TRAINING**

The Government may provide other training necessary to support mission requirements:

#### **1.3.2.1.1 SECURITY TRAINING**

The contractor shall provide initial and refresher security training to all employees, IAW Government regulations, local security policies, site-specific requirements, and classified debriefs to employees IAW 32 CFR Part 117, National Industrial Security Program Operating Manual (NISPOM Rule). The contractor should also be familiarized, and comply with, the DRSN and other applicable Security Classification Guides (SCG), to include annual refresher reviews.

#### **1.3.2.1.2. NETWORK USER TRAINING**

The contractor shall complete Network User Training by using <https://jkodirect.jten.mil> computer-based training prior to being granted access to the network infrastructure.

#### **1.3.2.1.3. MISSION-FOCUSED TRAINING**

The contractor shall complete all mission-focused training, e.g., Force Protection, Operational Security, Air Force Risk Management, Antiterrorism Awareness, etc., as directed by the COR.

### **1.3.2.2. EDUCATION, CERTIFICATIONS, AND WORK EXPERIENCE**

Cybersecurity personnel must possess a minimum of an Associate of Science Degree in Information Technology or Cybersecurity. The contractor shall ensure employees have, and maintain, required Information Technology or Cybersecurity education, training, or certifications IAW DoDM 8140.03 and current Government directives, regulations, and policies for the role, or labor category, it is fulfilling (reference DFARS 252.239-7001). Personnel are expected to possess Intermediate Level Cybersecurity Work Role experience. Any required education, certifications and work experience shall be obtained prior to any employee performing work under this contract. Personnel filling ISSO roles will have a minimum of four years of experience working RMF requirements and providing cybersecurity services. Employees deficient in these qualifications shall not be permitted to work under this contract.

### **1.3.2.3. TRAINING RECORDS**

The contractor shall maintain all training records for each employee. These shall be made available to the Government upon request.

### **1.3.3. SECURITY**

The contractor shall follow all security requirements (Operations and Communications Security) listed on the DD Form 254, Contract Security Classification Specification, to ensure information and documentation are protected. 32 CFR, Part 117, National Industrial Security Program Operating Manual (NISPOM) will be used as a guide.

#### **1.3.3.1. INSTALLATION ACCESS AND PHYSICAL SECURITY**

The contractor shall ensure that all employees authorized to work under this contract obtain installation access as required by DoDM 5200.08 Volume 3, Physical Security Program: Access to DoD Installations. The contractor shall also be able to obtain a Government Common Access Card (CAC) to perform the tasks associated with this requirement, in accordance with FAR Clause 5352.242-9001, Common Access Cards for Contractor Personnel. Contractor employees and property may be subject to search and seizure upon entering and leaving Government installations and facilities. Government-furnished identification shall be returned to the Government upon termination of an employee. Contractor employees shall comply with Government physical security plans at Government facilities. The contractor shall be responsible for any keys provided by the Government and be accountable for their use. Contractor employees shall not duplicate or provide keys to unauthorized personnel and shall implement procedures to prevent loss or misplacement.

#### **1.3.3.2. FACILITY SECURITY CLEARANCE (FCL)**

Prior to performance, the contractor shall possess an appropriate level FCL. The FCL certifies the contractor's ability to meet organizational clearances required for contract performance as indicated on the DD Form 254, Contract Security Classification Specification. The FCL requirement for the prime contractor includes those instances in which all classified access will be limited to subcontractors. No access to classified information shall be granted to contractor employees until a valid Interim or Final FCL has been granted by the Defense Counterintelligence and Security Agency. The contractor shall notify the 55 SCS Security Manager and COR that an Interim or Final FCL has been granted thirty (30) days prior to beginning on-site performance.

#### **1.3.3.3. PERSONNEL SECURITY CLEARANCE**

Contractors shall comply with current Government regulations, manuals, and policies to ensure all employees obtain the required background checks or security clearances equal to, or greater than, the classified information for which they are seeking access. The contractor shall fully cooperate with all security checks and investigations by furnishing requested information.

Contractor personnel shall possess a Top Secret (TS) clearance with SCI caveat. All contractors shall have the appropriate security clearance by contract award and obtain SCI caveat, NC2-ESI, within three (3) months. Due to the costs involved with security investigations, requests for contractor security clearances shall be kept to the absolute minimum necessary to perform service requirements.

#### **1.3.3.4. FACILITY ACCESS**

The contractor shall:

- a) Provide the 55 SCS Security Manager a Visitor Authorization Request (VAR) and comply with specific Government Information Systems Security Manager (ISSM) and host agency requirements for employees to gain access to specific Government facilities.
- b) Provide 55 WG/SSO a VAR with the words “PERM CERT” at the top for submission to USSTRATCOM/SSO for access to the USSTRATCOM building (for duration of contractor period of performance, or three years, whichever comes first).
- c) Provide an Entry Authorization List (EAL) to facility security managers and alarm monitoring agencies every six (6) months to gain access to limited access areas.
- d) Develop and maintain EALs for authorized personnel granted access to contractor-limited access areas and perform occasional escort duties for contractor workcenters.
- e) Comply with facility policies, instructions, and guidelines, e.g., Strategic Instruction on Foreign Travel Reporting, USSTRATCOM Personal Electronic Device (PED) Policy, USSTRATCOM SSO Handbook, etc.

#### **1.3.3.5. CONTRACTOR ACCESS**

The contractor shall:

- a) Immediately notify the 55 SCS Security Manager and COR when employees no longer require access and return all Government identification, access badges, and parking passes.
- b) Immediately notify the 55 SCS Security Manager and COR when Government identification and access badges are lost or stolen.
- c) Provide a monthly electronic spreadsheet of all employees and subcontractors supporting requirements on this PWS.

#### **1.3.3.6. PRIVACY ACT**

Performance on this contract requires that some personnel have access to Personally Identifiable Information (PII). Contractor personnel observe rules and regulations regarding physical security, breach reporting timelines, appropriate document handling, adherence to the Privacy Act of 1974, Title 5 of the U.S. Code, Section 552a, and other applicable agency rules and regulations.

#### **1.3.3.7. NO RIGHT TO PRIVACY**

All activities on DoW systems and networks may be monitored, intercepted, recorded, read, copied, or captured and disclosed by authorized personnel. There is no right of privacy on these systems. System personnel may give law enforcement officials any evidence of potential crime found on DoW computer systems. Use of these systems by any user, authorized or unauthorized, constitutes consent to monitoring, interception, recording, reading, copying, or capturing, and disclosure. The contractor shall report any unauthorized use to the ISSM.

#### **1.3.3.8. INFORMATION SECURITY (INFOSEC)**

All documents, schematics, drawings, presentations, email, graphs, web sites (to include all source code and items produced using any application-based editor, compiler software and/or operating system), User Data Module labels, and any hard or soft copy items produced or derived from the requirements of this PWS shall be marked with the classification markings and distribution statements as required in DoDM 5200.01 Volumes 1 through 4, *DoD Information Security Program*, DISAC 300-115-7, *Communications Security: Defense Red Switch Network Security Guidance*, and the Defense Red Switch Network Security Classification Guide. Distribution of

#### **1.3.3.9. SECURITY MANAGEMENT (TRANSMISSION OF CLASSIFIED MATERIAL)**

The contractor shall transmit and deliver classified material and reports IAW current Government manuals, regulations, and policies, i.e., DISAC 300-115-7.

#### **1.3.3.10. CLASSIFIED DESTRUCTION**

The contractor shall destroy classified material IAW current Government and local procedures. The Government will provide classified material burn bags and destruction shredders. Destruction facilities at USSTRATCOM are currently not available to tenant organizations.

### **1.3.4. QUALITY ASSURANCE MANAGEMENT**

The contractor shall ensure the quality, timeliness, and delivery of products and services within budget, and shall submit a Quality Assurance Plan within sixty (60) days of contract award. The contractor PM shall manage the contractor and any subcontractor employees, provide task direction and interface with the COR, PCO, and Government management. The contractor PM shall integrate and coordinate internal audits, inspections, and activities to ensure established policies and procedures are followed, in addition to maintaining an effective preventive and corrective action system, within normally scheduled duty hours. As such, expected and unexpected employee absences shall be managed by the contractor PM. Additionally, a continuity plan must be established to ensure no mission degradation in the event of employee turnover.

#### **1.3.4.1. PERFORMANCE MEETINGS**

When requested by the Government, the contractor shall attend regularly-scheduled or impromptu program, contract, and management in-person meetings, virtual meetings, and teleconferences to discuss any contractor performance issues not resolved by other means. The contractor shall notify and invite COR to any impromptu meetings, unless said meetings are deemed contractor-only. Any deficiencies identified by the COR shall be appropriately-addressed by the contractor within three (3) business days, or as agreed upon by Government representatives, dependent on issue complexity. If Government policy deviations are necessary, concurrence by COR, 55 SCS leadership, the PCO, DISA, or other relevant entities may be required.

#### **1.3.4.2. GOVERNMENT QUALITY ASSURANCE SURVEILLANCE PROGRAM**

The Government shall evaluate the contractor's performance under this contract in accordance with the Quality Assurance Surveillance Plan (QASP). This plan is primarily focused on what the Government must do to ensure the contractor has implemented PWS tasks in accordance with performance standards. It defines how the performance standards will be applied, the frequency of surveillance, and the minimum acceptable Performance Thresholds. The Government may inspect the Contractor using a QASP through random inspections, scheduled inspections, or any other method of inspection that the Government determines reflects the actual successful performance of this contract. Failure of the contractor to correct validated Government complaints will be considered a failure to perform. As part of the Government's Quality Assurance Program, the Government may:

- a. Review, and, if warranted, reject any reports or other submittals required of the contractor.
- b. Review performance and service records, including, if applicable, but not limited to, any computerized or hardcopy records maintained by the contractor documenting performance under this Contract, and require correction of any unsatisfactory conditions noted.
- c. Determine the adequacy of the Contractor's Quality Control Plan (QCP), documentation, and the overall success of this program. The Government may order improvements if it determines the programs are insufficient and/or ineffective.
- d. Obtain tenant satisfaction survey information and require improvements in service based on such information to the extent the results correlate with deficiencies in contract requirements.
- e. Conduct random and routine physical inspections of work products and systems, to include programs and files maintained in computers and contractor's onsite offices and work areas and require correction of any deficiencies noted.
- f. Perform inspections with Government personnel or independent third-party inspectors. 55 SCS/QA personnel may assist with inspections upon request.

#### **1.3.5. APPEARANCE AND STANDARDS OF CONDUCT**

The contractor shall ensure that its employee policy for standards of conduct and personal appearance foster a professional and safe work environment conforming to the Government's existing organizational culture. Contractor employees shall practice high standards of personal hygiene and maintain a clean, neat appearance while performing on this contract. The Contractor shall ensure

compliance with all applicable standards, handbooks, Air Force Manuals, Air Force Instructions, etc. Personnel shall always clearly display contractor identification badges, logoed shirts, etc.

Contractor employees who threaten the safety or welfare of the installation, or its personnel, may be immediately removed and/or barred from the installation. The COR, or designated Government representative, may require the contractor to remove any contractor employee from the job site for reasons of misconduct, security violations, or found to be, or suspected to be, under the influence of alcohol, drugs, or other incapacitating agent. The installation Commander has the authority to bar such individuals from the installation. Removal from the job site, or dismissal from the premises, shall not relieve the contractor of contract requirements. Any individual designated to be removed from the contract, as noted above, shall be replaced with a temporary employee within fourteen (14) calendar days and with a permanent employee within thirty (30) calendar days.

#### **1.3.6. CONTINUATION OF ESSENTIAL DOW CONTRACTOR SERVICES DURING CRISES**

The Government shall notify the contractor when contingencies and emergencies are declared. Special circumstances, or mission requirements, may preclude contractor personnel from departing facilities at normal close of business hours.

In crisis situations, to include times of war, on-base incidents, natural disasters, weather events, or other contingencies, as declared by base leadership, the National Command Authority, or Office of Personnel Management (OPM), the contractor must provide continuous cybersecurity services to support ongoing military missions. Within 180 days, the contractor shall develop a Continuity of Operations Plan (COOP).

#### **1.3.7. GOVERNMENT SITE RULES**

In the execution of duties on a Government installation, or in a Government building, the contractor shall fully comply with local military installation, city, state, and federal laws, regulations, and ordinances pertaining to performance of services required under this contract.

The contractor shall:

- a) Conform to all safety and security requirements.
- b) Observe all rules and regulations issued by the installation's Senior Official pertaining to fire, safety, sanitation, severe weather, access to the installation, and non-contract-related conduct.
- c) Take all reasonable steps and precautions to prevent accidents and preserve the life and health of all personnel associated in any way with the performance of this contract.
- d) Take any other immediate precautions for safety and accident prevention purposes.
- e) Report all safety mishaps and violations to the COR within eight (8) hours of occurrence.

### **1.3.8. PERIOD OF PERFORMANCE**

The period of performance shall be for one (1) base year and four (4) 12-month option years. The period of performance reads as follows:

Base Year	17 March 2026 – 16 March 2027
Option Year I	17 March 2027 – 16 March 2028
Option Year II	17 March 2028 – 16 March 2029
Option Year III	17 March 2029 – 16 March 2030
Option Year IV	17 March 2030 – 16 March 2031

## **2. CONTRACTOR CYBERSECURITY SUPPORT REQUIREMENTS**

This PWS defines cybersecurity task requirements for contractor performance in the areas outlined below:

- a. DRSN Cybersecurity Support
- b. Global Aircrew Strategic Network Terminal (G-ASNT) Cybersecurity Support
- c. Non-hardened Aircrew Alerting System (NAAS) – Klaxon Cybersecurity Support
- d. Other 55 SCS Cybersecurity Support
- e. TDY/Travel
- f. Government-furnished Property and Services

### **2.1. CLIN 001 DRSN CYBERSECURITY SUPPORT**

The contractor shall establish and continuously maintain the Authorization to Operate (ATO) for Offutt DRSN, related subsystems, as well as Offutt DRSN accreditation associated with segments of multiple NC3 systems that connect to Offutt DRSN, such as the Survivable Emergency Conferencing Network Digitization (SECN-DZ), Presidential and National Voice Conferencing (PNVC), various gateways, and long local communications circuits, in accordance with RMF guidelines; NIST 800-53, Rev 4, *Security and Privacy Controls for Federal Information Systems and Organizations*; Committee on National Security Systems Instruction No. 1253 (CNSSI 1253, Rev 4), *Security Categorization and Control Selection for National Security Systems*; DODI 8510.01, *Risk Management Framework for DoD Systems*; and DISAI 270-50-9, *Life Cycle Sustainment Planning*, among other risk management framework directives.

The contractor shall:

- a) Provide cybersecurity support services, as Information Systems Security Officers (ISSO), for the 55 SCS DRSN program.
- b) Provide assessments on the severity of weaknesses, or deficiencies, discovered in the local DRSN operations environment, and recommend corrective actions to address vulnerabilities.
- c) Use the RMF process to identify, analyze, and oversee risk in order to maintain an active Offutt AFB DRSN ATO.
- d) Process, store, maintain, update, and validate RMF documentation, in a classified network environment, for all DRSN-related programs.

- e) Assist in the configuration management process to maintain, update, and audit the DRSN network using methods and tools in accordance with DoW, AF, and local policies.
- f) Utilize Assured Compliance Assessment Solution (ACAS), or other DRSN DAO-approved scanning software, to accomplish audit controls.
- g) Complete monthly audit file backups of DRSN Administration Terminals.
- h) Establish appropriate Response Plans to the results of audit analyses for network security, as well as procedures for notification of associated entities, to include updating Response Plans annually.
- i) Participate in DRSN-related requirements discussions with stakeholders and devise cybersecurity solutions.
- j) Complete updates to the DRSN RMF packages in XACTA IA Manager during all steps of the RMF process.
- k) Develop, as necessary, DRSN Body of Evidence documents, including, but not limited to, Security Plans, Security Assessment Reports (SAR), Plan of Actions and Milestones (POAM), risk assessment reports, network diagrams, rack elevations, equipment inventories, software lists, and security controls traceability matrices.
- l) Develop, implement, assess, manage, and monitor DRSN security controls and RMF family policies.
- m) Update POAMs as required by the AFGSC and 16<sup>th</sup> Air Force (16 AF) Assessment and Authorization (A&A) Teams.
- n) Coordinate with the DRSN ISSM to implement changes within XACTA.
- o) Interface with ORSMO, USSTRATCOM, Defense Information Systems Agency (DISA), Air Combat Command (ACC), Delegated Authorizing Official (DAO), Defense Threat Reduction Agency (DTRA), Nuclear C3 Enterprise Center (NEC), DRSN long local circuit site representatives, U.S. Allies, and other stakeholders during the RMF package A&A process.
- p) Ensure monthly audit file backups of all secure and non-secure DSS-2A switches, ECCs, Admin Terminals, MTK's, etc., are accomplished, as appropriate, and document who has access to the equipment. Additionally, any equipment not requiring authentication, or waivers, must be documented.
- q) Document remote access capabilities and personnel with permissions such as DISA, O&M, and IA.
- r) Ensure physical security, personnel security, incident handling, training validation, other security awareness requirements, etc., have been satisfied by all DRSN users for continued network access.
- s) Schedule and complete quarterly destruction of media in accordance with USSTRATCOM and Offutt AFB policies.
- t) Sanitize, remove drives, and remove memory, as applicable, from hardware and ensure destruction is accomplished according to established Government and local security procedures.
- u) Work with DRSN O&M contractors and ORSMO in developing and maintaining Contractor Standard Operating Procedures required for ongoing RMF Accreditation Program.
- v) Assist in configuration management process reviews to establish procedures for ensuring contractor work instructions are continually updated and audited.
- w) Communicate with internal and client project team members, and work to influence teams regarding solution designs, processes, and approaches.
- x) Serve as the principal advisor in ensuring appropriate operational security posture for organizational mission and business systems.
- y) Manage and document A&A projects using XACTA IA Manager A&A workflow platform.
- z) Advise, conduct, and document risk assessments, develop System Security Plans (SSP), and create POAMs and security policies and procedures.

- aa) Advise and guide customers in the implementation of security controls, doctrine, and policies.
- bb) Participate in system discovery meetings to categorize systems for ATO purposes, as well as promote DRSN policy and process creation.
- cc) Obtain, manage, and file Sensitive Compartmentalized Information Facility (SCIF) and TEMPEST accreditation documents as part of the DRSN RMF Accreditation Program.
- dd) Implement cybersecurity standards and procedures to identify, report and resolve security violations.
- ee) Establish and satisfy cybersecurity requirements based upon user, policy, regulatory, and resource demands.
- ff) Integrate and implement computer system security solutions associated with DRSN to include, but not limited to, IP transition efforts, control LANs, Cyber Security Service Provider (CSSP) sensors, Enhanced Command Consoles, administrative terminals, Conference Management Agents (CMA), software upgrades, PNVC routers/switches, network gateways, etc.
- gg) Analyze general cybersecurity-related technical problems in conjunction with Offutt O&M, USSTRATCOM, DISA, 55 WG, and other organizations, and provide support in solving these issues.
- hh) Attend in-person or virtual regularly-scheduled or impromptu cybersecurity-related meetings, as required by the COR, and provide meeting minutes to support RMF requirements.
- ii) Provide applicable training to Offutt DRSN O&M and ORSMO in support of cybersecurity objectives.
- jj) Support cybersecurity audits by external Government agencies, as necessary.
- kk) Perform Special Security Representative (SSR) functions, as required by COR, for managing the security of the DRSN SCIFs and telecommunications closets, including oversight of any DRSN SCIF PED violations. The Government shall continue to maintain full SSR responsibility.
- ll) Assist with all hardware and software entry/exit requirements pertaining to USSTRATCOM, as dictated by USSTRATCOM policy.
- mm) Update any changes to documentation as an artifact in XACTA within three (3) business days.
- nn) Ensure precautions are in place such that other team members' XACTA data is not erroneously overwritten. ISSOs shall maintain copies of controls templates after each update.
- oo) Maintain artifacts specified within the RMF package such that they can be inspected by ORSMO semi-annually.
- pp) Ensure all security controls are reviewed and tested to complete the 3-year cycle per DAO requirements.
- qq) Quarterly maintain and update the Global Information Grid (GIG) Interconnection Approval Process (GIAP) VPN registry for DRSN long local circuits.
- rr) Manage all DRSN Memorandums of Agreement (MOA), Memorandums of Understanding (MOU), and Acknowledgement of Responsibility (AOR) Letters between Offutt DRSN and external customers for the DRSN RMF Accreditation Program. Update these documents annually and conduct complete reviews every three (3) years.
- ss) Courier classified equipment or media to approved destinations throughout Offutt AFB in accordance with applicable security regulations.
- tt) Update NC3 hardness checklists and fix-action responses to DTRA, NEC, and other audits from NC3 investigative entities.
- uu) Maintain a DRSN binder and electronic file folder on the appropriate computer network.
- vv) Coordinate drawing updates with Offutt DRSN O&M, and other organizations, as required.
- ww) Manage and continuously monitor DRSN cybersecurity programs to document and include any new requirements in the DRSN ATO.
- xx) Serve as cybersecurity consultants for ORSMO and DRSN O&M technicians.

- yy) Ensure incident handling, personnel/physical security, and security training/awareness requirements are also met by DRSN O&M personnel.
- zz) Validate the DRSN program for any new personnel training requirements, i.e., Juniper operating system, PNVC, G-ASNT, Klaxon training, etc.
  - aaa) Assist with escorting visitors at Offutt AFB DRSN, as authorized.
  - bbb) Provide the Government with Monthly Status Reports (MSR), outlining all Information Assurance (IA) work accomplished for that month, with out-of-cycle updates, as necessary.
  - ccc) Support other DRSN-related RMF accreditation tasks, as required.

## **2.2. CLIN 002 (55 WG) - GLOBAL AIRCREW STRATEGIC NETWORK TERMINAL (G-ASNT) CYBERSECURITY SUPPORT**

Contractor shall provide ISSO support for the ground portion of the Air Force Global Strike Command (AFGSC) Global Aircrew Strategic Network Terminal (G-ASNT) for the purpose of maintaining an ATO for 55 SCS equipment in the 55 WG Command Post and 55 SCS Tactical Radio transportable equipment. The G-ASNT system provides protected, robust communication capabilities to missile, nuclear bomber, and support aircraft crews in austere operational environments. The ISSO shall serve as a primary advisor to ensure an appropriate operational security posture meets day-to-day mission objectives.

The contractor shall:

- a) Provide cybersecurity support for building an initial RMF package to support the ATO for the ground element of the AFGSC Global Aircrew Strategic Network Terminal (G-ASNT) for the 55 SCS and 55 WG (Command Post)
- b) Develop technical solutions that require collaboration with the G-ASNT Program Management Office (PMO) and internal experts for deep analyses and understanding of impacts on end-products and solutions.
- c) Help resolve technical problems and mitigate programmatic issues that are unclear and require extensive technical knowledge.
- d) Serve as the principal advisor for Offutt AFB G-ASNT customers, ensuring appropriate operational security posture for organizational mission and business systems per the G-ASNT PMO.
- e) Advise on all matters involving RMF, A&A, and day-to-day security of NC3 mission systems.
- f) Manage and document A&A projects to provide inputs to the G-ASNT PMO for submission in the eMASS A&A workflow platform, or other platform, as dictated by the PMO.
- g) Document and track controls and artifacts using Microsoft Excel and other software products.
- h) Conduct audits on G-ASNT system.
- i) Advise, conduct, and document risk assessments, develop System Security Plans (SSP), POAMs, and security policies and procedures.
- j) Advise and guide customers in the implementation of security controls, doctrine, and policies.
- k) Implement cybersecurity standards and procedures to identify, report and resolve security violations.
- l) Establish and satisfy cybersecurity and security requirements based upon user, policy, regulatory, PMO, and resource demands.
- m) Integrate and implement computer system security solutions.
- n) Analyze general cybersecurity-related technical problems and provide support in solving these issues.

- o) Develop, review, and update Risk Management Framework Plan and supporting documentation to comply with NIST SP 800-53 requirements in support of the ATO.
- p) Attend in-person and virtual regularly-scheduled meetings, or impromptu cybersecurity-related meetings, as required.
- q) Report G-ASNT cybersecurity work in an MSR.
- r) Maintain a G-ASNT binder and electronic file folder on the appropriate computer network.
- s) Support other G-ASNT-related tasks, as required.

### **2.3. CLIN 003 (55 WG) - NON-HARDENED AIRCREW ALERTING SYSTEM (NAAS) – KLAXON CYBERSECURITY SUPPORT**

The contractor shall provide cybersecurity support for a Non-hardened Aircrew Alerting System (NAAS), owned and maintained by 55 SCS, but utilized by NAOC and 55 WG Command Post in support of NAOC and STRATCOM Alert Aircrew Mission. More commonly known as Klaxon, the system provides modern network-based non-hardened communications and notification capabilities to support aircrews at Offutt. The ISSOs shall serve as the primary cybersecurity advisors to establish the Klaxon ATO, and maintain the ATO as the system evolves.

The contractor shall:

- a) Provide cybersecurity support and accomplish tasks necessary for building an initial RMF package to support the ATO for the NAAS Klaxon.
- b) Provide cybersecurity support services for the 55 WG Command Post NAAS KLAXON system.
- c) Develop technical solutions that require deep analyses, collaboration with internal experts, and understanding of the impacts on the end-product solution.
- d) Solve technical problems and issues that are unclear and require appropriate technical knowledge.
- e) Serve as principal advisors in ensuring appropriate operational security posture for organizational mission systems.
- f) Advise on all matters involving the RMF, A&A, and day-to-day security of mission and business systems.
- g) Manage and document A&A projects using the appropriate IA Manager workflow platform.
- h) Develop, review, and update Risk Management Framework Plan and supporting documentation to comply with CNSSI 1253 requirements in support of the ATO.
- i) Advise, conduct, and document risk assessments, development of SSPs, POAMs, and security policies and procedures.
- j) Advise and guide customers in the implementation of security controls, doctrine, and policies.
- k) Implement cybersecurity security standards and procedures to identify, report and resolve security violations.
- l) Establish and satisfy cybersecurity and security requirements based upon user, policy, regulatory, and resource demands.
- m) Integrate and implement computer system security solutions as the system evolves.
- n) Analyze general cybersecurity-related technical problems and spearhead solving these problems.
- o) Report NAAS Klaxon cybersecurity-related work in an MSR.
- p) Support other 55 WG Command Post NAAS Klaxon system-related cybersecurity tasks, as required.

## **2.4. CLIN 004 - OTHER 55 SCS CYBERSECURITY SUPPORT**

The contractor Cybersecurity Team may support the 55th Strategic Communications Squadron in other cybersecurity-related matters. The contractor cybersecurity Subject Matter Experts (SME) shall serve as primary advisors, ensuring appropriate operational security posture for organizational mission and NC3 systems.

The contractor shall:

- a) Provide cybersecurity subject matter expertise for the 55 SCS, DRSN O&M, and mission partners in defining security requirements during the design and development process.
- b) Assist in developing technical solutions, specifications, and system designs that require collaboration with internal experts, extensive analyses, and understanding of impacts on end products and solutions.
- c) Assist in solving technical problems and issues that are unclear and require substantial technical knowledge.
- d) Serve as principal advisors on cybersecurity matters for organizational mission and business systems.
- e) Advise on all matters involving the RMF, A&A, and day-to-day security of mission and business systems.
- f) Manage and document A&A projects using XACTA IA Manager and eMASS A&A workflow platforms.
- g) Advise, conduct, and document risk assessments, develop SSPs, POAMs, and security policies and procedures.
- h) Advise and guide customers in the implementation of security controls, doctrine, and policies.
- i) Implement cybersecurity standards and procedures to identify, report and resolve security violations and other issues.
- j) Establish and satisfy cybersecurity and security requirements based upon user, policy, regulatory, and resource demands.
- k) Integrate and implement computer system security solutions.
- l) Analyze general cybersecurity-related technical problems and support in solving these problems.
- m) Report other cybersecurity work in the MSR.
- n) Support other 55 SCS cybersecurity efforts, as required.

### **2.4.1. OTHER TERMS OF SUPPORT**

In the event Offutt DRSN is reorganized under another Command, any non-DRSN IA functions shall be detached from this Offutt DRSN cybersecurity contract. Cybersecurity personnel supporting DRSN efforts would no longer be required to aid in non-DRSN IA tasks. If funded, cybersecurity support may continue separately under the appropriate CLIN, if appropriate, under the new Command. Additionally, the primary work location, Government-provided resources, and administrative support shall transfer to the different organization.

## **2.5. CLIN 005 - TDY/TRAVEL**

The contractor may be required to travel, on occasion, to attend DRSN-related Working Groups, IA-related conferences and symposiums, additional training, or to support remote site installations. The contractor shall comply with Federal Acquisition Regulation: 31.205-46 Travel Cost ([https://www.acquisition.gov/far/part-31#FAR\\_31\\_205\\_46](https://www.acquisition.gov/far/part-31#FAR_31_205_46)) requirements. Additionally, for any 55 SCS-funded travel, the contractor shall gain approval for mode of travel, lodging, and deployed means of conveyance (i.e. rental car) from the 55 SCS Travel Authorizing Official prior to departing for travel, and prior to making changes to previous approvals. Upon completion of travel, and prior to billing the government, the contractor shall submit travel vouchers for all travelers and provide receipts for all airfare, lodging, and any expense greater than \$75. The contractor shall submit travel reports, technical reports, or as-built drawings of DRSN equipment installations using standard base software, such as Microsoft Office products and MS Visio within five (5) working days.

## **3. GOVERNMENT-FURNISHED PROPERTY AND SERVICES**

The Government may provide the following Government Furnished Property (GFP):

### **3.1. GOVERNMENT FACILITIES**

The Government shall provide office space, storage space, desks, file cabinets, and facilities at each site. These facilities shall meet the requirements of the Occupational Safety and Health Act (OSHA). No hazards have been identified for which a work-around has not been established. The Government shall correct OSHA hazards in accordance with base-wide Government-developed and approved plans for abatement, considering safety and health priorities. Lack of prior identification of such conditions does not warrant or guarantee that no possible hazards exist, nor that work-around procedures will not be necessary, nor that the facilities, as furnished, will be adequate to meet the responsibilities of the contractor. Compliance with the OSHA and other applicable laws and regulations for employee protection is exclusively the contractor's obligation. The Government assumes no liability or responsibility for the contractor's compliance, or noncompliance, with such responsibilities, except for the responsibility to make corrections in accordance with approved plans of abatement, subject to base-wide priorities. Prior to any modification of the facilities by the contractor, the contractor shall notify Quality Assurance Personnel (QAP), authorized Government representative at the site, and the Procurement Contracting Officer (PCO), and provides documentation describing, in detail, the modifications requested. No alterations to the facilities shall be made without specific written permission from the PCO; however, in the case of alterations necessary for OSHA compliance, such permission is not unreasonably withheld. The contractor will return the facilities to the Government in the same condition as received, fair wear and tear and approved modifications excepted. The facilities are to be used for performance of this contract only.

### **3.2. GOVERNMENT PROPERTY**

The Government shall provide the contractor with a list of equipment utilized in support of the contract. Within fifteen (15) calendar days of contract award, and no sooner than thirty (30) calendar days prior to the contract completion, a joint inventory of equipment shall be conducted by the contractor and a Government representative. The Government reserves the right to require the contractor to sign for, and assume

accountability of, any CCSS equipment, or other GFP, for which it is providing Information Assurance support.

### **3.3. CONTRACTOR PROPERTY MANAGEMENT**

The contractor shall establish a property management plan and submit it to the PCO for approval within thirty (30) calendar days of contract award. The plan shall detail the contractors policies, procedures, and practices on how they will manage and safeguard the GFP for which they are responsible.

### **3.4. UTILITIES**

The Government shall furnish electricity, water, sewage, heating, and air conditioning for facilities, as required.

### **3.5. INSTALLATION MAIL DISTRIBUTION**

The Government shall provide on-base mail distribution service for official Government mail, except as authorized for OCONUS locations, required under terms of this PWS.

### **3.6. TELEPHONE**

The Government shall provide local phone service consisting of on-base services. The Government provides Defense Switched Network (DSN), long distance, and off-base local services, as required. Use is limited to matters related to the performance of this contract.

### **3.7. COMPUTER**

The Government shall provide Non-secure Internet Protocol Router Network (NIPRNet), Secure Internet Protocol Router Network (SIPRNet), and Joint Worldwide Intelligence Communications System (JWICS) access, if the Government deems the contractor requires access to those services to support this contract. The Government shall also provide access to all software required on said networks to support the contract. All IT services are limited to matters related to the performance of this contract.

### **3.8. FORMS AND PUBLICATIONS**

The Government shall provide all Government forms and publications expressly required by the contractor to perform the contract services. Contractor forms are acceptable; however, prior Government approval must be obtained before use.

### **3.9. REFUSE COLLECTION**

The Government shall provide refuse disposal for normal administrative functions.

### **3.10. INSECTS AND RODENT CONTROL**

The Government shall provide insect and rodent control for all Government facilities.

### **3.11. SECURITY POLICE**

The Government shall provide general on-base Security Police services. The appropriate telephone numbers shall be furnished by the Government.

### **3.12. BASE CIVIL ENGINEERING**

The Government shall provide fire prevention and protection services, including inspection and maintenance of Government-furnished fire extinguishers and systems.

### **3.13. EMERGENCY MEDICAL SERVICES**

The Government shall provide emergency medical treatment and emergency patient transportation service for contractor personnel on a reimbursable basis.

### **3.14. TRANSPORTATION**

Government transportation may be provided, subject to approval and amendment of this contract by the PCO. The transportation services will be limited to official Government business necessary for performance of this contract.

## **4. TECHNICAL DEFINITIONS**

The following technical terminology, acronyms, and references apply to this contract:

### **4.1. TECHNICAL TERMINOLOGY**

**Availability** - A measure of the degree to which an item is in an operable and committable state at the start of a mission when the mission is called for at an unknown (random) time.

**Bench Stock** - Consumable items utilized on a day-to-day basis (i.e.: wire, bulbs, printer paper, fuses, etc.).

**COMSEC (Communications Security) Material** – Item designed to secure or authenticate telecommunications. COMSEC material includes, but is not limited to key, equipment, devices, documents, firmware, or software that embodies or describes cryptographic logic and other items that perform COMSEC functions.

**Fault Management** - Fault management is defined as the detection, isolation, and correction of network problems.

**Government Property** - All property owned or leased by the Government. Government property includes both Government-furnished property and contractor-acquired property. Government property includes material, equipment, special tooling, special test equipment, and real property. Government property does not include intellectual property and software.

**Interfaces** - The junction or point of interconnection between two systems or equipment with different characteristics. They may differ with respect to voltage, frequency, operating speed, type of signal, and/or type of information coding.

**Isolation** - The action required to locate a failure within an equipment item using support or built-in test equipment.

**Line Replaceable Unit** - The lowest unit (part, circuit card, module, etc.) of a larger assembly authorized for replacement by on-site/organization level technicians.

**Maintenance** - All actions taken to retain material or equipment in a serviceable condition or to restore it to serviceability including inspection, adjustment, repair, rebuilding, and reclamation. All supply and repair actions taken to keep a site in condition to carry out its mission. The routine recurring work required to keep a facility or item of equipment in such condition that it may be continuously utilized at its designed capacity and efficiency for its intended purpose. All work shall be accomplished in accordance with Government and service-approved commercial publications and work specifications.

**Maintenance Documentation** - Technical manuals, user manuals, equipment schematics, and applicable microcode listings which are necessary to perform maintenance on the equipment.

**Network Management Subsystem** - The network management subsystem consists of a switch monitoring system known as Advanced RED Defense Switched Network (DSN) Information Management Support System (ARDIMSS), a network management system (NMS), and the telemetry network and call detail history collection and report generation components known as the Enhanced Switch Reporting System (ESRS). ARDIMSS is a Government-owned and contractor-maintained product. ARDIMSS software and

hardware are configuration controlled under a system-specific configuration management plan. The NMS is a commercial product. The telemetry network and call detail history ESRS is a combination of commercial products. Significant changes to the network management subsystem architecture are subject to DRSN CCB approval. Routine changes, modifications, and upgrades to the fielded ARDIMSS, NMS, and ESRS are controlled by the DRSN CCB Secretariat and coordinated with DISN and NetOps Center Configuration Control Boards (CCBs).

**On-Call Response** - Technician is not required to be physically present in the workcenter, however, must have a means of being contacted (telephone, beeper, etc.) so they can respond to outages within a specified time limit.

**Preventive Maintenance** - Maintenance performed by the contractor, which is designed to detect malfunctions in the equipment and keep the CCSS equipment and switches fully operational.

**Response Time** - The period which is measured as the elapsed time beginning with Government notification, that maintenance is required. Notification is the bona fide attempt by the Government to contact the contractor by telephone, pager, or other means. Response time shall be measured as the elapsed time from Government notification, until the contractor arrives at the work site.

**Site** - A predefined user location and the complement of CCSS equipment located on that Government installation.

**Switching Subsystem** - The switching subsystem consists of specialized, noncommercial RED and BLACK digital telephone switching systems that provide expanded Private Automatic Branch Exchange call features which include multilevel precedence and preemption (MLPP), hot lines, conferencing capability, and interfaces to other secure voice systems. The primary switching platform of the DRSN Switching Subsystem is the Raytheon Digital Small Switch (DSS-2A).

**TEMPEST (Telecommunications Electronics Materials Protected from Emanating Spurious Transmissions)** – An unclassified term referring to technical investigations, study, and control of compromising emanations from electrically operated information processing equipment (telecommunication and automated information systems equipment); these investigations are conducted in support of emanations and emissions security.

**Timing and Synchronization (T&S) Subsystem** - The T&S subsystem consists of a series of station clocks, clock distribution systems, filters, buffers, and cabling that provide stable T&S signals to the transmission and switching subsystem components. The timing signal quality and master or slave timing configurations between the T&S devices and the other network subsystems are governed by this Circular.

**Transmission Subsystem** - The transmission subsystem consists of a combination of Government furnished equipment (GFE) interfaced to the Defense Information Systems Network (DISN) transport layer and to commercially leased circuits. The DRSN Transmission Subsystem provides connectivity between DRSN RED switches, connectivity between a DRSN RED switch and users located remotely from the switch, and interconnections with other secure networks and systems.

## 4.2. ACRONYMS

<b>A&amp;A</b>	Assessments and Authorizations
<b>AETC</b>	Air Education and Training Command
<b>AFB</b>	Air Force Base
<b>AFMAN</b>	Air Force Manual
<b>APSR</b>	Accountable Property System of Record
<b>ARDIMSS</b>	Advanced RED Defense Switched Network Information Management Support System
<b>ASI</b>	Authorized Service Interruption
<b>CA/CRL</b>	Custodian Authorization/Custody Receipt Listing
<b>CCSD</b>	Command Communications Service Designator
<b>CCSS</b>	Command and Control Switching System
<b>CEU</b>	Channel Encryption Unit
<b>CFM</b>	Contractor Furnished Materials
<b>CG</b>	Communications Group
<b>CMA</b>	Conference Management Agent
<b>CMCS</b>	COMSEC Material Control System
<b>COCOM</b>	Combatant Command
<b>COMSEC</b>	Communications Security
<b>COR</b>	Contracting Officer's Representative
<b>CSR</b>	Customer Problem Report
<b>CRO</b>	COMSEC Responsible Officer
<b>DCO</b>	Defensive Cyberspace Operations
<b>DISA</b>	Defense Information System Agency
<b>DISAC</b>	Defense Information System Agency Circular
<b>DLADS</b>	Defense Logistics Agency Disposition Services
<b>DNC</b>	DISA NetOps Center
<b>DoD</b>	Department of Defense
<b>DoDD</b>	Department of Defense Directives
<b>DoDI</b>	Department of Defense Instructions
<b>DoDM</b>	Department of Defense Manuals
<b>DPAS</b>	Defense Property Accountability System
<b>DRSN</b>	Defense Red Switch Network
<b>DRSNOC</b>	Defense Red Switch Network Operation Center
<b>DSCS</b>	Defense Satellite Communication System
<b>DSS</b>	Digital Small Switch
<b>EAL</b>	Entry Authorization Letter
<b>EMP</b>	Electromagnetic Pulse
<b>DTRA</b>	Defense Threat Reduction Agency
<b>ECC</b>	Enhanced Command Console
<b>ECO</b>	Equipment Control Officer
<b>FCL</b>	Facility Security Clearance
<b>FLSO</b>	Field Logistic Support Office
<b>G-ASNT</b>	Global Aircrew Strategic Network Terminal
<b>GOC</b>	Global Operations Center
<b>GSO</b>	Government Service Owner
<b>IA</b>	Information Assurance
<b>IAW</b>	In Accordance With
<b>INFOSEC</b>	Information Security
<b>IP</b>	Internet Protocol

<b>IS</b>	Information System
<b>ISA</b>	Interconnection Security Agreement
<b>ISO</b>	International Organization for Standards
<b>ISPM</b>	Information Security Program Manager
<b>ISSO</b>	Information System Security Officer
<b>ISSM</b>	Information System Security Manager
<b>IST</b>	Integrated Services Telephone
<b>IT</b>	Information Technology
<b>ITER</b>	Information Technology Equipment Room
<b>ITI</b>	Interim Terminal Interface
<b>ITIL</b>	Information Technology Infrastructure Library
<b>IUID</b>	Item Unique Identification
<b>JWICS</b>	Joint Worldwide Intelligence Communications System
<b>Klaxon</b>	An electromechanical alerting device (same as NAAS)
<b>KMI</b>	Key Management Infrastructure
<b>KOA</b>	KMI Operating Account
<b>KOAM</b>	KMI Operating Account Manager
<b>LAN</b>	Local Area Network
<b>LRU</b>	Line Replaceable Unit
<b>MAJCOM</b>	Major Command
<b>MDA</b>	Multifunction Digital Adapter
<b>MILDEP</b>	Military Department
<b>MO</b>	Management Office
<b>MSD</b>	Multi-stream Summing Device
<b>MSR</b>	Monthly Status Report
<b>NAAS</b>	Non-Hardened Aircrew Alerting System (same as Klaxon)
<b>NAOC</b>	National Airborne Operations Center
<b>NATO</b>	North Atlantic Treaty Organization
<b>NC2-ESI</b>	Nuclear Command and Control – Extremely Sensitive Information
<b>NC3</b>	Nuclear Command, Control, and Communications
<b>NCA</b>	National Command Authority
<b>NGA</b>	National Geospatial-Intelligence Agency
<b>NIPRNet</b>	Non-Secure Internet Protocol Router Network
<b>NISPOM</b>	National Industrial Security Program Operating Manual
<b>NMCC</b>	National Military Command Center
<b>NMS</b>	Network Management Subsystem
<b>NOC</b>	Network Operating Center
<b>NSA</b>	National Security Agency
<b>O&amp;M</b>	Operations and Maintenance
<b>OCONUS</b>	Outside Continental United States
<b>OPM</b>	Office of Personnel Management
<b>ORSMO</b>	Offutt Red Switch Management Office
<b>OSD</b>	Office of the Secretary of Defense
<b>OSHA</b>	Occupational Safety and Health Act
<b>PC</b>	Property Custodian
<b>PCC</b>	PNVC Communications Console
<b>PCO</b>	Procurement Contracting Officer
<b>PD</b>	PNVC Display
<b>PDS</b>	Protected Distribution System
<b>PII</b>	Personally Identifiable Information

<b>PMI</b>	Preventative Maintenance Inspection
<b>PMO</b>	Project Management Office
<b>POAM</b>	Plan of Action and Milestones
<b>POC</b>	Point of Contact
<b>PoP</b>	Period of Performance
<b>PSI</b>	PNVC Speaker Interface
<b>PWS</b>	Performance Work Statement
<b>PNVC</b>	Presidential and National Voice Conferencing
<b>QA</b>	Quality Assurance
<b>QAP</b>	Quality Assurance Personnel
<b>QASP</b>	Quality Assurance Surveillance Plan
<b>RFC</b>	Request for Change
<b>RMF</b>	Risk Management Framework
<b>RSU</b>	Remote Switching Unit
<b>SCI</b>	Sensitive Compartmented Information
<b>SCS</b>	Strategic Communication Squadron
<b>SDS</b>	Secure Digital Switch
<b>SECN-DZ</b>	Survivable Emergency Conference Network - Digitization
<b>SIA</b>	Security Impact Analysis
<b>SIPRNet</b>	Secure Internet Protocol Router Network
<b>SRG</b>	Site Responsibility Guide
<b>SSR</b>	Special Security Representative
<b>STE</b>	Secure Telephone Equipment
<b>SVRO</b>	Secure Voice Responsible Officer
<b>TPI</b>	Two Person Integrity
<b>TRS</b>	Training Squadron
<b>TS</b>	Top Secret
<b>UAPO</b>	Unit Accountable Property Officer
<b>UMUX</b>	Universal Digital Loop Transceiver (UDLT) Multiplexer
<b>VAR</b>	Visitor Authorization Request
<b>VDD</b>	Version Description Document
<b>VoIP</b>	Voice over Internet Protocol
<b>WG</b>	Wing
<b>WGCP</b>	Wing Command Post
<b>WHCA</b>	White House Communications Agency
<b>WWSVCS</b>	Worldwide Secure Voice Conferencing System

#### **4.3. REFERENCE DOCUMENTS**

Contractor must always utilize the most recent editions of references, unless dictated to follow previous editions. The Government ISSM should be informed by contractor of any changes to references that may impact customers, any aspects of security, or contractor performance.

<b><u>Reference Document #</u></b>	<b><u>Publication Name</u></b>
<b>32 CFR, Part 117</b>	National Industrial Security Program Operating Manual (NISPOM)
<b>OAFB IEMP 10-2</b>	Offutt AFB Installation Emergency Management Plan
<b>DFARS 252.239-7001</b>	Information Assurance Contractor Training and Certification
<b>DISAC 300-115-7</b>	Communications Security: DRSN Security Guidance
<b>DISAC 300-115-8</b>	DRSN Security Management
<b>DISAC 300-115-70</b>	DRSN Security Classification Guide
<b>DISAC 310-70-84</b>	DRSN IP Network Management Guide
<b>DISAC 310-70-86</b>	DRSN Configuration Management Guide
<b>CJCSI 6211.02D</b>	Chairman of the Joint Chiefs of Staff Instruction Defense Information Systems Network (DISN) Responsibilities
<b>AFI 17-130</b>	Cybersecurity Program Management
<b>AFMAN 17-1203</b>	Information Technology Asset Management (ITAM)
<b>AFMAN 17-1302-O</b>	Communications Security (COMSEC) Operations
<b>DoD 8570.01-M</b>	Information Assurance Workforce Improvement Program
<b>DoDD 5400.07</b>	Freedom of Information Act Program
<b>DoDD 8140.01</b>	Cyberspace Workforce Management
<b>DoDI 8500.01</b>	Cybersecurity
<b>DoDI 8523.01</b>	Communications Security
<b>DoDM 5200.01 Volumes 1-4</b>	DoD Information Security Program
<b>DoDM 5200.08 Vol 3</b>	Physical Security Program
<b>FAR Clause 5352.242-9001</b>	Contractor Common Access Cards
<b>ISO 9000</b>	Accountability and Management of DoD Equipment and Other Accountable Property
<b>ISO 20000</b>	Cybersecurity-IT Service Management
<b>Title 5 of the U.S. Code, Section 552a</b>	Privacy Act of 1974
<b>DRSN IP Operations &amp; Maintenance Guides</b>	Information Technology
<b>N/A</b>	Multifunction Digital Adapter (MDA) User Guide
<b>N/A</b>	DRSN Long Local Over IP Network Subscriber Design and Installation Guide
<b>N/A</b>	Raytheon Integrated Services Telephone Version 2 User Guide
<b>N/A</b>	SECN-DZ Site Responsibility Guide