AIR FORCE RESEARCH LABORATORY

ROME RESEARCH SITE

ROME, NEW YORK

PERFORMANCE WORK STATEMENT

FOR

CORPORATE FACILITIES RESEARCH SUSTAINMENT

PCSN G-8-2018

2 June 2018

(Contract Number FA8751-18-X-XXXX)

TABLE OF CONTENTS

SECTION	DESCRIPTION	PAGE
1.0	OBJECTIVE, SCOPE AND BACKGROUND	3
2.0	DESCRIPTION OF SERVICES	3
3.0	SERVICES SUMMARY	7
4.0	GOVERNMENT-FURNISHED PROPERTY, BASE SUPPORT, AND SERVICES	10
5.0	GENERAL REQUIREMENTS	12

1.0 OBJECTIVE, SCOPE AND BACKGROUND.

1.1 The objective of this effort is to ensure the availability, reliability, and security of the Information Systems (IS) and networks described herein.
1.2 The scope of this effort is to fulfill technical, administrative, and security requirements to include implementation of technical information for security policies; maintenance of specified hardware and software with regard to Information Assurance (IA), Information Technology (IT), Configuration Management (CM); Risk Management Framework (RMF), Software Management; and engineering solutions, providing technical input to Research and Development (R&D) processes from an IT and IA perspective.

1.3 Background.

1.3.1 AFRL/RIG mission is to “lead the research, development and integration of affordable information exploitation and cyber technologies for transition to our air, space and cyberspace forces.” As such, devoted expertise in systems engineering, cyber security (information assurance), network management, configuration management, and software management are required to address these challenges, as well as to accelerate AFRL’s ability to put new capabilities in the hands of warfighters. This mission presents unique and diverse challenges.

1.3.2 Conducting air, space and cyber research and development daily operations is a complex task, especially in terms of interpreting and applying computer and network security procedures in a fluid, mix-mode[1] environment.

1.3.3 This effort shall provide solutions and expertise that balance the need for innovation with the need for robust security approaches and procedures, as well as attending to the myriad of associated details found within such a diverse environment.

2.0 DESCRIPTION OF SERVICES. The Contractor shall accomplish the following:

2.1 Implement Technical Information Security Procedures.

2.1.1 Provide knowledge and analysis for development, configuration, handling and disposal - “hands- on”- of resources utilized in all aspects of state-of-the-art R&D technologies.

2.1.2 Identify and research technical implications that arise, working with the Contracting Officer’s Representative (COR) through resolution.

2.1.3 Apply and utilize security classification guides and program protection plans with COR for protection of critical program information, data and equipment.

2.1.4 Identify to the COR any security risks associated with introduction and operation of hardware and network infrastructure. To include comingling of hardware, data exposure (erasure) and destruction thereof.

2.1.5 Assist the COR in formulation of mitigating procedures for policy development for secure operations of secure facilities.

2.1.6 Identify to the COR any security risks associated with software utilization on hardware and network infrastructure, to include mitigation of Cybersecurity identified vulnerabilities.

2.2 Provide accountability for all associated hardware and software for Corporate Facilities, including research areas, at COR discretion.

2.2.1 Maintain configuration management and software management (including license use), on R&D systems and networks, while building integrated services.

2.2.2 Maintain the unique R&D environment(s) whilst anticipating unique requirements and challenges in performing functions within both classified and unclassified environments.

2.2.3 Maintain documentation for security, information assurance, software, computer access control, as required by COR, applicable to regulations, policies and procedures, including Operating Plan (OP) changes.

2.2.4 Provide ongoing assessment to COR to maintain TEMPEST (formerly EMSEC), Operations Security (OPSEC), Computer Security (COMPUSEC) and physical security requirements.

2.2.5 Maintain pertinent DoD, AF, and local regulations, procedures and policies with regard to daily operations. Interact with COR to resolve unique problems and situations.

2.2.6 Review new and existing AF Instructions (AFIs), Time Compliance Network Orders (TCNOs), and Network Tasking Orders (NTOs); implement change actions, as identified by the COR. Identify impacts to R&D operations, including software management, configuration management, network management and information assurance that may impact daily operations.

2.2.7 Maintain scheduling of activities for Corporate Facilities through Share Point calendars; visitor clearance verifications utilizing the Joint Personnel Adjudication System (JPAS) (or other approved local security resources), and Agenda\Attendee Worksheet(s).

2.2.8 Maintain Corporate Facilities organizational mailboxes (i.e. RRS.CCF.STAFF, RIG USLM and RIG SUPPORT for program and project requirements, Risk Management Framework package coordination and daily operations.

2.2.9 Provide changes to RRS Help Desk (i.e. Customer Support (RIOS) for Share Point Division Division sites in coordination with the COR.

2.2.10 Provide DRAFT, AF Form 3215, Communications-Computer Systems Requirements Document (CSRD) and AF Form 332, Base Civil Engineer Work Request, for corporate facilities and division R & D environments, in coordination with the COR. Track form(s) signed by the COR, including metrics, until completion of submitted request(s).

2.2.11 Maintain Corporate Facilities (i.e. CCF & COTF) internal access control lists.

2.2.11.1 Validate access control list semi-annually with the RRS Security Office (AFRL/RIOF).

2.2.12 Provide Risk Management Framework packages for Corporate Facilities and COR identified division R & D areas.

2.2.12.1 RMF packages shall be coordinated with the Division Cyber Security Liaison (CSL) for acceptance and digital signature prior to staffing to Cybersecurity Office (AFRL/RIOS).

2.2.12.2 RMF submitted packages will be tracked in the AFRL/RCC RMF Portal with monthly status provided to Division CSL and COR, as a minimum.

2.2.13 Maintain remenance security for corporate facilities including division R & D secure areas with Corporate Facilities Manager coordination.

2.2.14 Maintain Corporate Facilities internal worksheets for audit purposes. Worksheets are to be maintained for equipment moves, equipment remenance and other areas as identified by Corporate Facilities Manager.

2.2.15 Maintain Corporate Facilities (CCF & COTF) Front Desk entry/exit control during operating hours.

2.2.15.1 Maintain media entry/exit control, including virus scanning, assigning of media control number(s), retrieval of stored media, shipments; prevent “piggy backing” of personnel; and entry/removal of hardware.

2.3 Provide information assurance solutions and technical input to R&D processes.
2.3.1 Maintain R & D environments; including associated hardware and software, with IA solutions and provide technical solutions to R&D processes from an IT and Cybersecurity perspective.

2.3.2 Maintain information systems for Corporate Facilities, including division R & D areas as identified by COR.

2.3.3 Maintain network enclave for Corporate Facilities, including division R & D areas as identified by COR.

2.3.3.1 Maintain network enclave configurations, to include access control lists, firewalls, route table configurations, access accounts, etc. Configurations will be maintained at the security level of the enclave, to include standalone systems.

2.4 Maintain Unit Software License Management (USLM) for all information systems utilized by RIG Division.

2.4.1 Coordinate division USLM activities with the Base SLM (BSLM), Division Software License Managers, Cyber Security Liaisons, Program Managers, Division Management Office, end-users, and purchaser(s) of software, including licenses.

2.4.2 Maintain the accuracy of Corporate Facilities, and division R & D areas, for software license entry in RRS database (i.e. SamDB, or other database as identified by BSLM).

2.4.3 Maintain controlled delivery of all software to end-user, including entry of purchase (or reuse) in identified database.

2.4.4 Perform a semi-annual and annual inventory of all software licenses and cross-check with installed software on information systems throughout Corporate Facilities, including identified division R & D areas by the COR. Report the results to the COR and Division CSL, as a minimum.

2.4.5 Maintain a soft copy of the software license inventory and "Proof-of-License Ownership" of all Government-owned and Commercial-Off-The-Shelf (COTS) software in use within Corporate Facilities, and division R & D identified areas by the COR. Proof may consist of hardcopy or softcopy documentation from the supplier such as manuals, purchase documentation, email(s), or distribution media via web sources.

2.4.5.1 Hard copy may be maintained for classified areas, but shall be minimized as much as possible.

2.4.6 Maintain any physical inventory of license agreements or licenses (e.g. purchase documentation) and physical software media (e.g. user manuals, Compact Disc Read-Only Memory Discs (CD-ROMs), and Digital Video Discs (DVDs), in a centralized location, under lock, controlled access (e.g., locked drawer, file cabinet, room, etc.) approved by the COR.

2.4.7 Identify software that does not have associated licenses; resolve with Division CSL and COR by assembly of proofs-of- purchase and request replacement license(s) from publishers.

2.4.7.1 Identify if apparent replacement licenses, media, etc. will generate new cost(s). If this is identified, coordinate with Program Manager for JON/PCSN.

2.4.7.2 Provide information to purchaser once requirements are met. Courtesy copy Division CSL and COR when CSRD submission is done.

2.4.8 Provide files to the local Functional Area Record Manager or the Base Records Management Office (RIOSI) to ensure proper retention and disposition of official records and records approval.

2.4.8.1 Maintain local files for Corporate Facilities, as required by the COR, for daily operations.

2.4.9 Provide training, as well as recommendations, to Government and Contractor personnel to maintain information systems, in compliance.

2.4.10 Provide SLM status reports. (See CDRLs, A003, B003 and C003)

2.4.10.1 Maintain internal spreadsheet of deviations from approved software license policy.

2.4.10.2 Identify POA&M dates, in coordination with the COR, for compliance.

2.4.11 Provide software to RIG personnel once required actions are completed to ensure proper controls for end use.

2.5 Program Management.

2.5.1 Report progress toward accomplishment of contract requirements. (See CDRLs, A001, B001 and C001)

2.5.1.1 Maintain changes for information systems, including MTO, TCNO, IAVA resolutions. Identify to COR, as needed, activities requiring extensive tracking (i.e. Windows 10 Migration, etc.).

2.5.2 Conduct oral presentations at such times and places as specified in the contract schedule, or as specified by the COR. Provide the status of technical progress made to date in performance of the contract. (See CDRLs, A002, B002 and C002)

2.5.2.1 Provide IT, IA, CM, software and related solutions by Contractor ability to perform in a time constrained manner.

2.5.3 Continuity Book.

2.5.3.1 Maintain a continuity book that outlines the policies and procedures utilized to accomplish the requirements of the PWS. Provide updates and supplements during the course of the contract. Include technical progress while working with various directorate Programs and Program Managers. (See CDRLs, A004, B004 and C004)

2.5.4 Technical work accomplished and information gained during performance of this acquisition will be documented. Include all pertinent observations, nature of problems, positive and negative results, and design criteria established, where applicable. Document procedures followed, processes developed, i.e. “Lessons Learned”. Document the details of all techniques and procedures used in evolving technology or processes developed. Cross-reference separate design, engineering, or process specifications delivered to permit a full understanding of the total acquisition. (See CDRLs, A005, B005 and C005)

2.6 Foreign Disclosure.

2.6.1 Provide research and analyses of technical, operational, policy, and political and military factors for proposed international programs with Foreign Disclosure Officer coordination.

2.6.1.1 Analyses shall include collection of information for Foreign Disclosure Officer determinations.

2.6.2 Provide services for drafting justifications such as coordination of disclosure guidance for international programs with Foreign Disclosure Officer coordination.

2.6.2.1 Analyses shall include AFMC Form 191, AFMC Form 193, AFMC Form 458, One-Time, or other analyses as identified by the Chief, Foreign Disclosure.

2.6.3 Provide administrative functions such as coordination of disclosure initiatives and record keeping related to disclosure activities and determination with Foreign Disclosure officer coordination.

2.6.3.1 Maintain Foreign Disclosure Spreadsheet, as provided by the Chief, Foreign Disclosure, for all foreign disclosure activities, to include determinations.

2.6.4 Provide metrics to AFLCMC/WFNJ (Command, Foreign Disclosure), on a monthly basis, with inclusion of the Chief, Foreign Disclosure and COR.

2.6.5 Maintain a Foreign Visit System, SPAN account, for Foreign Visit Request coordination.

2.6.5.1 Provide local staffing of Foreign Visit Request(s), via SPAN, to include local worksheets with sponsor, with Foreign Disclosure officer coordination.

2.6.6 Conduct monthly Foreign Disclosure orientation training with Foreign Disclosure Officer coordination.

2.6.6.1 Conduct training, for special interest Foreign Disclosure areas, as identified by Chief, Foreign Disclosure and COR (i.e. OCONUS Travel, etc.).

3.0 SERVICES SUMMARY (SS). The contract service requirements are summarized in performance objectives. The performance threshold briefly describes the minimally acceptable levels of service required for each requirement. The SS and the Contractor's Quality Control Plan provide information on contract requirements, the expected level of Contractor performance, and the expected method of Government validation and confirmation of services provided. These thresholds are critical to mission success. Procedures as set forth in the contract Inspection/Acceptance clause will be used to remedy all deficiencies.

Identifier	Performance Objective	PWS Paragraph	Performance Threshold

SS1	Fulfill all technical requirements at the identified facilities. Performance will be assessed through review of: • Corporate Facility Worksheets (Metrics) • Risk Management Framework: Boundary Diagram(s), Hardware List(s), CIS(s); TEMPEST (formerly EMSEC) physical layout diagrams, Hardware List(s); and Authority to Operate/Connect required documentation • USLM database entries to include software tracking, changes, updates and license usage • Troubleshooting efforts to resolve problems during time critical testing, development and demonstration	2.2 2.2.4 2.4 2.2.6	Exceptional = 0 deficiencies. Very Good = 1-2 functionally unrelated deficiencies. Satisfactory = 2 functionally related or 3 functionally unrelated deficiencies. Marginal = either 4 or more functionally unrelated deficiencies or 3 functionally related deficiencies. Corrective action acceptable to the COR is planned or underway. Unsatisfactory = either 4 or more functionally unrelated deficiencies or 4+ functionally related deficiencies. Corrective action acceptable to the COR is not planned or underway.
SS2	Quality Program Maintenance – Monthly Status Report	2.5.1	Exceptional = On time with no rework Very Good = On time with minimal rework Satisfactory = Less than 2 working days late with no to minimal rework Marginal = Less than 2 working days late with major rework Unsatisfactory = Anything other than above
SS3	Quality Program Maintenance – Oral Presentation(s)	2.5.2	Exceptional = On time with no rework Very Good = On time with minimal rework Satisfactory = Less than 2 working days late with no to minimal rework Marginal = Less than 2 working days late with major rework Unsatisfactory = Anything other than above
Identifier	Performance Objective	PWS Paragraph	Performance Threshold

SS4	Quality Program Maintenance – Technical Report(s)	2.5.4	Exceptional = On time with no rework Very Good = On time with minimal rework Satisfactory = Less than 2 working days late with no to minimal rework Marginal = Less than 2 working days late with major rework Unsatisfactory = Anything other than above
SS5	Quality Program Maintenance – Continuity Book(s)	2.5.3	Exceptional = On time with no rework Very Good = On time with minimal rework Satisfactory = Less than 2 working days late with no to minimal rework Marginal = Less than 2 working days late with major rework Unsatisfactory = Anything other than above
SS6	Compliance with established security requirements	DD Form 254 and 5.2	Satisfactory = 0 deficiencies Unsatisfactory = 1 or more deficiencies

3.1 Quality Control. The Contractor shall develop and maintain a Quality Control program to ensure services are performed in accordance with commonly accepted practices and quality of service. Develop and implement procedures to identify and prevent performance deficiencies. As a minimum, develop quality control procedures addressing the areas identified in the Services Summary.

3.2 Quality Assurance. The Government will evaluate the Contractor's performance through periodic surveillance and customer feedback. The Government may inspect each task as completed or increase/decrease the number of inspections as appropriate. The Contractor shall initially validate customer feedback. The Government will make final determination of the validity of customer feedback in cases of disagreement or conflict.

3.3 Performance Deficiency. The Government will evaluate the Contractor’s performance to ensure services meet contract requirements. When a performance threshold has not been met or Contractor performance has not been accomplished, the COR will consider such an event as a performance deficiency and provide the Contracting Officer a Corrective Action Report (CAR) or similar documentation. The COR and Contracting Officer will objectively evaluate observed deficiencies and, if validated, notify the Contractor. The Contractor shall respond to the Contracting Officer in accordance with instructions provided and within 10 calendar days of receipt. Responses from the Contractor will be considered prior to the final decision made by the Contracting Officer.

3.4 Periodic Progress Meetings. The Contractor shall periodically meet with the COR, Contracting Officer, and other Government personnel as appropriate, to discuss the Contractor’s performance. The Contractor shall be prepared to discuss: Opportunities to improve the contract, modifications required of the contract, unsatisfactory inspections and trends against each

performance objective observed, positive performance, Contractor feedback, and steps taken by the Contractor to prevent unsatisfactory inspections and customer complaints, provide insight into any identified trends, and propose possible solutions. The minutes of these meetings will be signed by the CO, distributed to Government personnel and the Contractor. Should the Contractor not concur with the minutes, the Contractor shall provide a written notification to the CO identifying areas of non-concurrence for resolution.

3.5 Inspections, Evaluations, and Reviews by Other Government Personnel. The Contractor shall permit Department of Defense inspection visits, host installation visits, other required functional reviews, evaluations or inspections and staff assistance visits as required by the Government, to include MAJCOMs, Defense Information Systems Agency, Air Force Audit Agency, Inspector General Office, General Accounting Office or other Government agencies. Inspectors or inspection teams may make unannounced visits and will be provided unescorted access to facilities and equipment. The Contractor will be given the purpose of the visit and copies of any reports created. The Contractor shall take necessary actions and coordinate with the Government to resolve any discrepancies found as part of these inspections.

4.0 GOVERNMENT-FURNISHED PROPERTY, BASE SUPPORT AND SERVICES

4.1 The Contractor may use “common” computers in Corporate Facilities (i.e. Cafés, Front Desk, Foreign Disclosure Office, otherwise, no Government property shall be furnished.

4.2 The Contractor may use regularly available utilities and services to perform this contract, including the following:

4.2.1 Utilities. Reasonable and conservative use of electricity, water, sewage, heating/cooling, and computer connectivity.

4.2.2 Postal. On-site distribution, USPS and FedEx service limited to official Government mail matters required to perform this contract.

4.2.3 Installation Distribution. The Contractor shall process administrative communications for on-site transmission and comply with pouch service and official mail handling procedures. When transmitting classified mail, the Contractor shall adhere strictly to DoD 5220.22-M. The Contractor may use the inter-office mail to process and deliver administrative communications and containers between distribution offices and organizations on RRS.

4.2.4 Standard Form 65B or 65C, US Government Messenger Envelope, will be addressed with the office symbol.

4.2.5 The Contractor may use the inter-office mail for delivery and pick up of mail and small parcels. The inter-office mail function shall not be used for Contractor company mail and postage for company mail. The return address on all official Government mail dispatched in the performance of the contract shall contain the Contractor's name followed by the applicable functional address symbol.

4.2.6 Telephone with connectivity outside of RRS for official use only, including local, long distance and Defense Switching Network (DSN). Telephone service is subject to monitoring.

4.2.7 Custodial Service. Provided through an existing contract.

4.2.8 Refuse Collection. Bulk refuse collection is provided through an existing contract. Refuse will be limited to those items authorized in the refuse collection contract and generated in the performance of this contract.

4.2.9 Real Property Maintenance. The Government will maintain and repair real property facilities. The Contractor will call Civil Engineering to request maintenance and repair of real property.

4.2.10 Civil Engineering. The Government provides fire prevention and protection for the site, including inspection and maintenance of Government fire extinguishers and systems, as well as pest control and grounds maintenance. The Fire Department telephone extension is 911 (Rome Fire Department) for emergencies and 330-2961 (RRS Security) for routine calls.

4.2.11 Security Police. The Government provides general on-base Security Police service for the site.

4.2.12 Information Technology Equipment. To request IT capabilities, prepare and submit an AF Form 3215, Communications-Computer Systems Requirements Document. The Rome Research Site RIOS office provides communications and computing services. The Help Desk can be reached at 330-7275 for customer service, communication-computer systems trouble call support, and assistance requests.

4.2.13 Equipment Maintenance. Send requests for equipment maintenance to the Logistics Materiel Control Activity (LMCA).

4.2.14 Printing and Duplicating Services. Request printing and duplicating using DD Form 844, Requisition for Local Duplicating Service.

4.2.15 Internet, Servers, Local Area Networks (LAN). Internet, servers, and LAN shall be used only for Official Government Business to perform this contract. The Contractor shall submit a DD Form 2875, System Authorization Access Request (or local equivalent form), for each person requiring a network account and/or access to e-mail, the Internet, and other provided network services. DOD 52002.R, Para 3.614 and Appendix K require, as a minimum, a National Agency Check for all personnel before being allowed access to unclassified Air Force computer systems. All individuals must complete mandatory IA training prior to access, this training shall be documented and reported to the Directorate’s Information Systems Security Officer. In addition, System Administrators may implement measures to limit access to information required to perform duties. Systems are subject to monitoring.

5.0 GENERAL INFORMATION

5.1 Contractor Employees.

5.1.1 The Contractor shall not employ persons for work on this contract identified by the Contracting Officer as a potential threat to the health, safety, security, general well-being, or operational mission of the installation and its population.

5.1.2 The Contractor shall not employ any person who is an employee of the United States Government if the employment of that person would create a conflict of interest, or an appearance of a conflict of interest. When employing off-duty Air Force military personnel, the Contractor shall comply with AFI 64-106, paragraph 3. In the event it becomes necessary to replace any contract personnel, the Contractor shall not be reimbursed for costs associated with such removal including the costs for replacement of any personnel so removed.

5.1.3 The Contractor is prohibited from employing off-duty Government personnel who are responsible for surveillance of any contracts/subcontracts awarded to the Contractor.

5.1.4 The Contractor shall inform the Contracting Officer in writing within five (5) working days of any incidents of misconduct by their employees that violate laws of the US. Incidents that may lead to problems between Rome Research Site and local Government officials must also be reported within five (5) workdays.

5.1.5 The Contractor shall be responsible for obtaining any necessary licenses and permits to comply with any applicable U.S., state, and local laws, codes, and regulations. Ensure that employees have current and valid professional certifications before starting work as required (to include DoD 8570/8140 compliance).

5.1.6 Contractor employees involved in the performance of this contract, must complete, and provide, to the Contracting Officer, a Non-Disclosure Agreement.

5.1.7 The Contractor shall provide personnel who are qualified at the beginning of their work under this contract and who meet the minimum criteria for their respective labor categories, as those categories are defined in the underlying contract vehicle used to establish this contract.

5.1.8 Vacancies. The Contractor shall “back-fill” positions with qualified personnel to ensure all performance objectives are fulfilled without performance degradation. If a change of personnel occurs, the Contractor must ensure a replacement is hired and in place, with complete Common Access Card access and clearance (prior to the departure of the incumbent, unless impossible). If a vacancy is anticipated to exceed 30 calendar days, the Contractor shall provide a written plan acceptable to the COR and Contracting Officer describing how the vacancy will be filled or otherwise resolved.

5.1.9 Training. The Contractor shall ensure all employees provided under this contract are current in all training required to fulfill the requirements of this work statement.

5.1.9.1 Maintain an individual training record for each employee that includes a listing of all training completed by employee. Provide to the Government, for inspection, when requested.

5.1.9.2 Ensuring contractor personnel complete, within mandated time requirements, all initial and recurring mandatory training, such as the Cybersecurity (formerly Information Assurance) training, all required site general training, and any specialized training required to meet position specific requirements. The contractor will be responsible for all training except government unique training requirements. Additional unique government requirements will be negotiated on a case by case basis.

5.2 Security.

5.2.1 Personnel Security.

5.2.1.1 Contractor personnel must be citizens of the USA.

5.2.1.2 Prior to the start of the contract performance period, sufficient personnel will have the appropriate security clearances to perform the requirements specified in this work statement.

5.2.1.3 Contractor personnel shall hold a SECRET clearance, or an interim SECRET clearance that will lead to a successfully awarded SECRET clearance. Any personnel not requiring a SECRET clearance will undergo a National Agency Check with Inquiries (NACI) investigation, at minimum.

5.2.1.4 Apply for new personnel security clearances within thirty (30) days. Inform the COR in writing when the clearance is finalized so that familiarization with work procedures can be accomplished.

5.2.1.5 Comply with the requirements in DoD 5200.2-R Personnel Security Program (paragraphs 3-614, 3-401, and Appendix K) and AFI 33-119 Air Force Messaging (paragraph 3) before operating a Local Area Network or automated information system.

5.2.1.6 Personnel that require physical access to RRS shall be subject to criminal history check, national agency checks, and verification of identify. Either of these checks or the verification may result in costs being charged to those Contractor employees.

5.2.1.7 When it has been determined which Contractor will accomplish the project, a Visit Request from the company, preferably on Company letterhead, will be necessary prior to initial work commencement. The Visit Request letter needs to be signed by the Company President or Director of Human Resources. The Visit Request will also be used as the Entry Authority List. The Contractor will supply the Visit Request to Security (AFRL/RIOF) through the Contracting Office. The Visit Request can be done via RRS Visit Request Form, AFMC Form 97 or a simple Company Letterhead letter identifying all personnel who will be employed during the work. The request will contain a full name to include a middle initial (Frank A. Dude), date of birth (14 Dec 1953), state of driver’s license issuance and place of birth (Austin, Texas). This information will be used to do a Local Files Check. This check will provide Driver’s License Information, Wants & Warrants and Protection Orders and information on Illegal Immigration and suspected terrorist affiliations. The Local Files Check shall be accomplished prior to work commencing. If the individual is not a US Citizen they will not be allowed within the complex or facilities. If, the individual is not a US Citizen but has a Green Card, Form I-551 or has the I-551 stamp on their passport, Security will

need to see either one. There will be no foreign national workers allowed on the Rome Research Site. Provide the Company's phone number and a Project Leaders or Supervisor/Foremen cell-phone number is necessary for the Law Enforcement Desk Sergeant.

5.2.1.8 All facilities are entered using a magnetic media entry badge and PIN number. Contractor work within the facilities will be required to obtain an Unescorted Visitor Badge; this will be procured by the Division/Branch with oversight of the work. The badge is obtained in the lobby of Bldg. 3, West Wing, Security Office. This badge will be worn at all times within the facility. These badges will be returned to the Contracting Officers' Representative before completion of the final inspection. Any badges lost during the period of work will be reported to Security immediately.

5.2.1.9 Access to the RRS Complex is controlled by a Main Gate on Brooks Rd, located just west of the Otis & Brooks intersection. Identification for the Contractor to enter with a vehicle will be an access list supported by the electronic badge issued. All commercial vehicles entering the gate will be searched. One-time deliveries can be escorted from the gate to delivery point by project personnel.

5.2.1.10 All commercial vehicles are searched prior to entry into the RRS Complex. Vehicle operators will be aware of the vehicle search pull-off area prior to approaching the Main Gate. A search of the vehicle will be conducted prior to its entry. All vehicles not needed for delivery of equipment or tools will be parked in the visitor parking area unless cleared through Security. There are No vehicles allowed within 25 meters (80 ft.) of the RRS facilities.

5.2.1.11 All personnel should be aware that the Rome Research Site is Property of the United States Air Force. All personnel will follow all posted signage.

5.2.1.12 Contractor personnel will be notified by RRS Police of any emergencies which would require an evacuation or work stoppage, such as an increase in the Force Protection Condition.

5.2.1.14 The work to be done on this project is located in and around areas that are under the scrutiny of the Department of Defense Police assigned to the RRS Information Directorate. To gain access to the areas to examine the work to be done for job estimation purposes, arrangements must be made through the Contracting Office. Contractor personnel will be escorted into the areas for the purpose of project estimation. 5.2.2 Safeguarding Classified Information.

5.2.2.1 Conform to the provisions of DoD 5220.22-M National Industrial Security Program Operating Manual (NISPOM) for safeguarding classified information and provide for obtaining the security clearances required for Contractor and subcontractor employees requiring access to classified information. Only those persons who have the proper security clearance and a "need to know" will be given access to classified information or material.

5.2.2.2 Contractor personnel shall handle/process classified/unclassified material IAW DoD 5220.22-M National Industrial Security Program Operating Manual (NISPOM), DoD 5200.1R Information Security Program Regulation and AFI 31-401 Information Security Program Management.

5.2.3 Facility Security. Conform to the provisions of DoD 5220.22-M NISPOM regarding facility security.

5.2.4 The Contractor shall sign an agreement stipulating the security requirements of this contract as provided for in AFI 31-601, Industrial Security Program Management.

5.2.5 Personnel with access to Air Force computer systems (stand-alone or networked) shall comply with AFI 33-119, Air Force Messaging, and AFSSI 5027, Air Force Systems Security Instruction.

5.2.6 Building/Room Keys, RRS Access Badges, and Department of Defense Common Access Card (CAC).

5.2.6.1 Building/Room Keys. Personnel may be issued building/room keys. Immediately report any occurrences of lost or duplicated keys to the COR. In the event that keys are lost or duplicated, the Contractor shall, upon direction of the Contracting Officer, re-key or replace the affected lock(s) without cost to the Government. If the Contractor needs access to area(s) that are locked (i.e. mechanical rooms, janitor's closet, etc.), a request for entry of at least 2 working days prior to the need for access will be submitted to AFRL/RIOC construction representative. The area(s) will be provided access on a case by case or daily basis. The area(s) will be locked down at the end of the days' work.

5.2.6.2 RRS Access. All personnel will be issued a DoD Common Access Card. Personnel shall wear the CAC Card on the outer clothing, on the front of the body between the neck and waist so that the Card is conspicuously visible at all times. All badges shall be turned in upon termination of employment or completion of contract.

5.2.6.3 DoD Common Access Card. Access to certain facilities and the RRS computer network requires a CAC. The issuance of CACs will be at Government expense. Access to classified or restricted areas may include additional requirements. Maintain familiarity with local procedures for allowing access to RRS and comply with all access requirements. CAC cards must be returned upon completion of the contract or earlier if the need has dissipated, for example, through termination of any employee. The capability of a potential employee being allowed access should be considered in all hiring and subcontracting decisions. The U.S. Air Force will not be responsible or liable for a Contractor's employee being denied issue of a CAC or access to RRS. These requirements may in some respect be in addition to those identified in Air Force Federal Acquisition Regulation Supplement (AFFARS) 5352.242-9000 Contractor Access to Air Force Installations and they also will be subject to the withholding provision.

5.2.6.4 Keys, Common Access Cards, and RRS Badges. Develop, document, and implement procedures in the Quality Control Plan that ensure control and accountability for all keys, Common Access Cards, and RRS Access Badges issued to Contractor personnel. Include procedures for turn in of keys, Common Access Cards, and RRS Access Badges by personnel who no longer require access or upon termination or contract completion. Ensure keys, Common Access Cards, and RRS Access Badges are not lost, misplaced, or duplicated and are not used by unauthorized persons.

5.2.7 Physical Security. Secure work areas, property, and materials at the close of each work day. Conform to the provisions of AFI 31-101, AF Installation Security Program, for safeguarding all Government facilities, equipment, and material contained therein. Complete and document end-ofday security checks using Standard Form 701, as required.

5.2.8 Information Assurance. Maintain computer system integrity in accordance with the Air Force Computer Security (COMPUSEC) program. Comply with and apply the principles, criteria, policy and procedures specified in DoD 5200.28, Security Requirements for Automated Information Systems (AISs), DOD 8570.01-M, DoD Directives Systems Procedures, AFI 33-202, Computer Security, AACI 33- 201, Information Assurance, AFI 33-119, Air Force Messaging, AFI 33-129, Transmission of Information VIA the Internet, and AFI 33-112, Computer Systems Management, AFRL/RI Computer Security Management directives, as well as any supplements to these documents. Contractor personnel shall maintain OS and Security certification, and shall be on DoD accredited site of registered professionals.

5.3 Hours of Operation. The core hours established for Rome Research Site are 0600-1800 Eastern Standard Time. The Contractor normally will fulfill contract requirements during the hours specified for each functional area. The Contractor may work, with prior approval of the Contracting Officer, extended hours to ensure timely completion of work at no additional cost to the Government. When determined by the COR that the mission of AFRL/RI will not be adversely affected, the Contractor may be invited to participate in team- building activities with AFRL/RI personnel.

5.4 Discontinuation of Contractor Services during a Temporary Site-Level Closing. All services to be performed under the contract have been determined to be non-essential for performance during a temporary site-level closing. The site could be closed because of security problems, adverse weather, a site disaster or a local disaster, or other events that would necessitate the closing/delaying of base activities. Should any one of these situations occur the Contractor should listen to or watch one of the local television or radio stations for notification of a possible base closure/delay. The Contractor will not receive any other form of notification of a site closure from the Government, unless contacted by the Contracting Officer or the COR. The Contractor is responsible for notifying his/ her employees. The Contractor may call the RRS weather number, 330-3100, for the daily reporting procedure status.

5.5 Contract Holidays. The Federal Government observes the following holidays:

- New Year’s Day - January 1 (except weekends, then it will be either Monday or Friday)
- Martin Luther King’s Birthday - 3rd Monday in January
- President’s Day - 3rd Monday in February
- Memorial Day - Last Monday in May
- Independence Day - July 4 (except weekends, then it will be either Monday or Friday)

- Labor Day - 1st Monday in September
- Columbus Day - 2nd Monday in October
- Veteran's Day - November 11 (except weekends, then it will be either Monday or Friday)
- Thanksgiving Day - 4th Thursday in November
- Christmas Day - December 25 (except weekends, then it will be either Monday or Friday)

5.5.1 In addition to the federal holidays identified above, the AFRL Site Director may limit access due to emergency conditions. These events may include such things as inclement weather conditions, power outages, and/or other unexpected emergency situations. The Director will announce through public channels either delayed reporting or closure of RRS facilities due to emergency conditions. This announcement is made solely for safety and security purposes and to inform all personnel (Government and Contractor) of site closure/delayed reporting. The Director is not authorizing time off for Contractor employees and is not authorizing payment for work not performed. Contractors shall take all appropriate actions to notify their employees of closure/delayed reporting and make alternate work/schedule arrangements, if necessary.

5.5.2 The above applies to emergency situations only. Facilities will remain open for Contractor personnel during unscheduled federal closures (e.g., National Day of Mourning) or other instances where Government employees are granted administrative leave in non-emergency situations.

5.6 Phase Out/Transition.

5.6.1 In the event a follow-on contract is awarded to other than the incumbent, the incumbent Contractor will cooperate to the extent required to permit an orderly transition to the successful Contractor. During the phase-out familiarization period, the incumbent will be fully responsible for the performance of tasks and duties described herein. The Government reserves the right to conduct site visits in all facilities in conjunction with the solicitation of offers for the follow-on contract. With regard to the successor Contractor's access to incumbent employees, a recruitment notice may be placed in each facility.

5.7 Safety

5.7.1 The Contractor shall comply with all safety and health requirements necessary for the protection of personnel, facilities and equipment including, but not limited to, the Occupational Safety and Health Act (OSHA) (Public Law 91-596) and all applicable OSHA standards, while performing this contract at the Air Force Research Laboratory (AFRL), Rome Research Site (RRS), Rome NY. It is the Contractor's sole responsibility to make certain that all safety requirements are met.

5.7.1.1 Maintain a written safety program for compliance with the applicable OSHA standards, and make said plan available for review by the Government upon request by the Contracting Officer.

5.7.1.2 In the event of a mishap, or a "near miss", during the performance of this contract at AFRL RRS, notify the Contracting Officer or the AFRL RRS Safety Office in an expeditious manner. Written notification shall be provided to the Contracting Officer (who will forward a copy to the AFRL Safety Office) within 72 hours and shall include the following information (AF Form 978, Supervisor's Mishap Report, may be used):

a. Contract, Contract number, Name and Title of Person(s) Reporting
b. Date, Time and exact location of accident/incident
c. Brief Narrative of accident/incident (events leading to accident/incident)
d. Cause of accident/incident (if known)
e. Type of injuries resulting from the accident/incident and estimated cost of accident/incident (material and labor to replace/repair)
f. Nomenclature of equipment involved in accident/incident
g. Personnel involved in accident/incident
h. Corrective Actions (taken or proposed)
i. Other pertinent information

5.7.2 AFRL RRS uses a Safety and Health Management System (SHMS) to implement and manage its safety programs. A SHMS is a systematic approach to managing safety and health activities by integrating occupational safety and health programs, policies, and objectives into organizational policies and procedures. Simply stated, a SHMS is a set of safety and health program components that interact in an organized way. An effective SHMS consists of five critical elements that apply safety and health management practices of employers who have been successful in protecting the safety and health of their employees. All contractors are required to familiarize themselves with the requirements of a SHMS. An example of a SHMS is OSHA's Voluntary Protection Program (VPP). Detailed information on VPP is available at the OSHA website at http://www.osha.gov/dcsp/vpp/index.html. On-site contractors are required to attend a Local Conditions Course as part of in-processing at AFRL RRS.

5.7.3 If contractor or subcontractor employees work more than 1,000 hours per quarter on-site at the AFRL, Rome Research Site (RRS), and are required by OSHA to maintain injury and illness recordkeeping, then the following safety paragraphs below apply.

5.7.3.1 Submit Total Case Incidence Rate (TCIR) and Days Away, Restricted and/or Transfer Case Incident (DART) Rate and an OSHA Form 300A, Annual Summary of Work-Related Injuries and Illnesses, to the DET 4 Safety Office by 15 January each year. AFRL RRS will consolidate and submit this information as part of the installation's annual VPP Safety and Health Management Report. The TCIR is the total number of recordable injuries and illness cases per 100 full-time employees that a site has experienced in a given time frame. The DART rate is the number of recordable injuries and illness cases per 100 full-time employees resulting in days away

from work, restricted work activity, and/or job transfer that a site has experienced in a given time frame.

5.7.3.2 Submit a copy of your Safety and Health Program and corresponding site safety checklist to the Contracting Officer within 10 days after contract award. The program shall include appropriate measures to ensure the contractor reacts promptly to investigate, correct and track alleged safety & health violations and/or uncontrolled hazards in contractor work areas.

5.7.3.2.1 Include the name and phone number of the person who will be the primary point of contact for safety and health issues for the on-site operation. Keep the contract safety manager information current by notifying the Contracting Officer of any change in personnel or contact information.

5.7.3.2.2 Demonstrate a management commitment to employee safety and health; 5.7.3.2.3 Identify the application of the safety and health program to subcontractors;

5.7.3.2.4 Identify the roles and responsibilities of:

a) Management
b) Supervisors
c) Employees
d) Safety Coordinator

5.7.3.2.5 Identify applicable safety rules and regulations;

5.7.3.2.6 Include a worksite hazard analysis to include base-line hazard identification and required control measures;

5.7.3.2.7 Include a job site analysis to include hazards of tasks required to control measures;

5.7.3.2.8 Identify employee safety and health training requirements and the documentation process;

5.7.3.2.9 Include a workplace inspection frequency, to include identifying the individual conducting the inspections;

5.7.3.2.10 Include employee hazard reporting procedures;

5.7.3.2.11 Identify individual(s) responsible for corrective action of hazards;

5.7.3.2.12 Identify first aid/injury procedures;

5.7.3.2.13 Identify procedures for accident investigation and reporting;

5.7.3.2.14 Identify emergency response procedures; and

5.7.3.2.15 Identify the process for tracking controlled hazards in contractor work areas.

5.7.3.2.16 Identify disciplinary methods that will be used to discourage willful or repeated noncompliance by employees.

5.7.4 The contractor is responsible for establishing these requirements for all subcontractors whose employees work more than 1,000 hours per quarter during a calendar year at AFRL RRS.

5.7.5 Identify the processes and procedures that will be used to track compliance with the Safety and Health Program and correct violations in the Quality Control Plan.

5.8 REGARDING ACCESS TO AIR FORCE FACILITIES AND GOVERNMENT INFORMATION TECHNOLOGY NETWORKS.

5.8.1 Contractor employees requiring access to USAF bases, AFRL facilities, and/or access to U.S. Government Information Technology (IT) networks in connection with the work on this contract must be U.S. citizens. For the purpose of base and network access, possession of a permanent resident card (“Green Card”) does not equate to U.S. citizenship. This requirement does not apply to foreign nationals approved by the U.S. Department of Defense or U.S. State Department under international personnel exchange agreements with foreign governments. Any waivers to this requirement must be granted in writing by the Contracting Officer prior to providing access. The above requirement(s) are in addition to any other contract requirements related to obtaining a Common Access Card (CAC).

5.8.2 For purposes of paragraph 5.8.1 above, if an IT network/system does not require AFRL to endorse a contractor’s application to said network/system in order to gain access, the organization operating the IT network/system is responsible for controlling access to its system. If an IT network/system requires an U.S. Government sponsor to endorse the application in order for access to the IT network/system; AFRL will only endorse the following types of applications; consistent with the requirements above:

(1) Contractor employees who are U.S. citizens performing work under this contract.

(2) Contractor employees who are non-U.S. citizens and who have been granted a waiver.

(END PERFORMANCE WORK STATEMENT)