Attachment 2

AIR NATIONAL GUARD TELECOMMUTING WORK AGREEMENT

A2.1. Telecommuter agrees to adhere to the directed laws, policies, and procedures of the telecommuting program. Telecommuter recognizes that the telecommuting arrangement is not a right but a complementary tool the ANG may use to accomplish work.

Figure A2.1. Telecommuting Work Agreement.

The following constitutes an agreement between:_____ And _____ agree to Supervisor/Approval Authority Telecommuter the terms and conditions of the telecommuting program. The supervisor and telecommuter agree: Telecommuting schedule_____ Fixed_____ As needed

A2.2. The telecommuter will meet with the approval authority/supervisor to develop and/or amend performance agreements for work performed away from the official duty station. The telecommuter will complete all assigned work according to work procedures mutually agreed upon by the telecommuter and the approval authority/supervisor in the agreement.

A2.3. Participation in telecommuting does not change the telecommuter's official duty work location.

A2.4. Where applicable, the telecommuter agrees to document and submit to the supervisor/approval authority for endorsement, any changes in the work agreement.

A2.5. The telecommuter must ensure that a safe and healthy work environment exists. If required by the supervisor/approval authority, the telecommuter agrees to sign a self-certification checklist that proclaims the alternative work site is free of work related safety and health hazards.

Figure A2.2. Alternate Worksite.

The alternate worksite is: _____

A2.6. Any data, document or work product developed in telecommuter's telecommuting is the sole property of the United States Government.

A2.7. During telecommuting the supervisor/approval authority may check progress via telephone calls, electronic mail or other available means.

A2.8. The telecommuter agrees not to conduct personal business while in official duty status at the telecommuting workplace (e.g., caring for dependents, making home repairs, etc.).

A2.9. The telecommuter acknowledges that while telecommuting, he/she is subject to the applicable laws, regulations and instructions during the duty hours specified relative to the duty status.

A2.10. Equipment.

A2.10.1. The Government retains ownership and control of all hardware, software, and data associated with government-owned systems.

A2.10.2. Government equipment is FOR OFFICIAL USE ONLY. Installation, repair, and maintenance are at the sole discretion and direction of the issuing organization.

A2.10.3. The telecommuter agrees to protect any government-owned equipment, to prevent the use by others, and to use the equipment only for official purposes.

A2.10.4. The telecommuter agrees to install, service and maintain any privately owned equipment at the telecommuter's sole risk and responsibility. NOTE: Regular telecommuters accessing full network resources must use government furnished equipment.

A2.10.5. The government does not incur any cost or liability resulting from the use, misuse, loss, theft or destruction of privately owned computer equipment or resources. NOTE: Regular telecommuters accessing full network resources must use government furnished equipment.

A2.10.6. The telecommuter must comply with DoD, AF and ANG security procedures and ensure that security measures are in place to protect the equipment from damage, theft or access by unauthorized individuals.

A2.10.7. Access to sensitive documents, data, records, etc. on government equipment must be consistent with all DoD, AF and ANG directives and instructions. Privately owned equipment may not be used to access or view classified information. Users must remove any sensitive government information (e.g., Privacy Act, FOUO) from privately owned systems using an approved data removal method when the session is terminated.

A2.10.8. The telecommuter is responsible for providing security against loss due to malicious logic, physical or virus loss, theft, or damage. Anti-virus software is available for both government and privately owned computers.

A2.10.9. Telecommuters must provide adequate and timely access to their equipment for troubleshooting, installation, inventory, modification, etc., in the event an information handling incident is encountered and to ensure telecommuting guidelines are being followed.

A2.10.10. Telecommuters will only access network resources through approved gateway protocols and methods in accordance with NGB/A6 Remote Network Access Policy. Remote access guidelines apply to both government and privately owned equipment. NOTE: Direct connections to the network by privately owned equipment are prohibited.

A2.11. If telecommuting is no longer required or appropriate, the telecommuter must immediately return government-owned hardware, software, data and return all documents, project details and deliverables.

A2.11.1. Specific telecommuting project details:

A2.11.2. Scope of work (Description of project).

A2.11.3. Projected deliverables:

A2.11.4. Estimated amount of time to complete the project:

A2.11.5. Projected start and end dates:

A2.11.6. Type of duty:

A2.11.7. Number of estimated days/periods of duty (orders required for active duty):

A2.11.8. Individual's resource requirements:

A2.11.9. Progress report requirements:

A2.11.10. Additional remarks:

Figure A2.3. Additional Remarks.

Telecommuter Signature: _____ Date: _____
Supervisors Signature: _____ Date: _____
Approval Authority Signature: _____ Date: _____