Enclosure 4 – USAG Fort Bliss Telework Policy
Use of Government Furnished Equipment

1. The determination to provide and install government-furnished equipment for use by a teleworker at the alternate worksite is at the discretion of the Director/Support Office Chief.

a. Each organization will coordinate the service and maintenance of government-furnished equipment issued to their employees who telework.

b. Government-furnished equipment is provided to a teleworker for authorized U.S. Government use only and will be accounted for by the issuing organization. Family members and friends of the teleworker are not authorized to use any government-furnished equipment.

c. Government-furnished computer equipment, software, and communication devices, with appropriate security measures, are required for remote work with unclassified data (including controlled unclassified, and Privacy Act-protected data), when the access method involves a direct connection to the Headquarters Enterprise network, such as through the virtual private network or remote access server. In addition, the use of government- furnished equipment must comply with the appropriate provision. The employee must agree to comply with the terms of any computer software license and copyright agreements, as well as with any Army computer virus protection requirement and procedures.

d. Employee will use a government-furnished computer, the common access card (CAC) will be used to enable, cryptographic logon entry into information technology (IT) systems and applications that reside on DoD computer networks and systems. The CAC will also be the primary platform for implementation of public key infrastructure.

e. Telework employees will comply with all security provisions.

f. Telework employees are responsible for protecting any government furnished equipment and property at the alternative worksite. Employees will return all government-furnished equipment to organization property book officer or designated representative on the termination of employment relationship, the termination of the telework arrangement, or at the organization's request.

2. Telework employees are responsible for safeguarding all official information and data as required by applicable laws and regulations.

a. Classified information (hardcopy or electronic) will not be removed from the traditional worksite to an alternative worksite. No classified documents (hardcopy or electronic) may be taken to, or created at, an employee's alternative worksite. Controlled unclassified information may be taken to an alternative worksite, provided the employee takes necessary precautions to protect the data consistent with Army and DoD directives, regulations, and policies.

b. With a view to preventing the loss of any official information or data, the supervisor will determine how frequently, if at all, a telework employee must back-up copies of official information or data on OneDrive or designated TEAMS site. The supervisor may

require the employee to send backup copies of information or data to the traditional worksite.

c. Telework employees will apply approved safeguards to protect official information and data from unauthorized disclosure or damage and will comply with the Privacy Act of 1974 and implementing regulations.

3. The supervisor or other representative of the employee's organization retains the right to inspect the alternative worksite to ensure that safety standards are met and government-furnished equipment is properly maintained. When the employee's alternative worksite is in the employee's home, such inspections will occur by appointment only.

4. A telework employee remains subject to the provisions of the Joint Ethics Regulation, the general principles of Federal employment, and all other Federal and agency standards of conduct while working at the alternative worksite.