User Agreement Addendum and Education, Training, and Awareness Information:

By signing for my account, I am acknowledging the following:

1. Networked computer systems are increasingly essential to the successful performance of the USTRANSCOM mission. I have a personnel responsibility to help protect the information resident on USTRANSCOM networks. This responsibility includes abiding by applicable DoD and USTRANSCOM policies meant to protect said information.
2. As a member of a DoD Combatant Command, I am a target of malicious cyber actors. I must be cautious when reading e-mail or browsing the internet.
3. Portable Electronic Devices (PEDs) and cameras will not be connected to any USTRANSCOM system under any circumstances. PEDs include, but are not limited to: removable storage devices, phones, digital music players, Personal Digital Assistants (PDAs). Additionally, PEDs and cameras are prohibited from entrance to USTRANSCOM buildings in most circumstances under USTRANSCOM's Security Program.
4. IAW CYBERCOM orders, personnel may not transfer data from a classified machine to a machine of lower classification without an approved waiver, a two person integrity check, and an automated classification check with the appropriate tool. Contact your Directorate's security manager for more information.
5. In order to make sure security patches and configurations are being applied, all workstations must be re-started daily.
6. All software must go through a test and evaluation process before being installed on a workstation. Contact your office's FACCSM or Unit Requirements Officer (URO) for more details.
7. If you experience any IT issues or notice suspicious activity on your workstation, contact the Comm. Focal Point at 256-2666 or your office's FACCSM.
8. Information sent to a foreign user must meet the criteria for release and be appropriately marked. Contact your Directorate Foreign Disclosure Representative or the Command Foreign Disclosure Office (TCJ2-FDO, 220-7343 or 220-7164) for additional information.
9. I will report possible information systems security incidents as soon as they happen or are discovered to USTRANSCOM/J6-GCCC, 229-4222, or the Security Service Center/J3-FP, 220-6550.
10. I can contact my office FACCSM, the GCCC, or the Information Assurance Manager (IAM, 229-4049) for additional information.

_____ _____

User Name User Signature\Date