User Agreement Addendum and Education, Training, and Awareness Information

By signing for my account, I acknowledge the following:

1. I understand that networked computer systems and other communication devices are essential to the successful performance of the USTRANSCOM mission. I have an official personal responsibility to help protect the information resident on USTRANSCOM devices and networks. I must help protect USTRANSCOM Information Technology (IT) from tampering, theft or loss, taking care to protect any portable electronic devices and media such as laptops, cell phones, tablets, disks, and other authorized portable electronic storage media. This responsibility includes abiding by applicable DOD and USTRANSCOM policies meant to protect said information.

2. I understand that as a member of a DOD Combatant Command, I am a target of malicious cyber actors. I must be cautious when reading e-mail, responding to e-mails, and browsing the Internet.

3. I will operate all government-issued equipment and information systems in accordance with DOD 5500.7-R, "Joint Ethics Regulation (JER)," paragraphs 2-301 and 2-302.

4. I understand that if my government-issued devices are lost or stolen, I must immediately report the loss to the USTRANSCOM Protection Service Center (618-817-6550) and USTRANSCOM IT Service Desk (618-817-6432)/Joint Enabling Capabilities Command (JECC) Help Desk (757-278-7272).

5. I will restart my computing devices daily to apply security patches and configurations. If notified by an on-screen alert that a patch or update failed, I will immediately submit a ticket through the "MyIT" service portal or contact the IT Service Desk.

6. I will not connect my personally owned Portable Electronic Devices (PEDs) or peripheral devices to any USTRANSCOM system or network under any circumstances. Pursuant to USTCI 5700.07, "Policy for Information Security," PEDs include cellular/personal communications system devices (e.g., cellphones), laptop computers, wearable fitness devices (e.g., Fitbits), two-way pagers, audio/video recording devices, wireless messaging devices, e-readers (e.g., Kindles), tablets (e.g., iPads), smart watches, personal digital assistants (PDAs), blackberries, mp3 players (e.g., iPods), medical devices, cameras, universal serial bus (USB) removable storage devices, printers, scanners, and other similar devices capable of receiving, transmitting or storing information. Peripheral devices include wired and wireless keyboards, mice, hubs, and headsets/ear buds.

7. I will not bring personally owned PEDs or peripheral devices into areas of USTRANSCOM used to process classified information. I understand that individual waivers for specific models of personal fitness monitoring devices can be requested from USTRANSCOM Protection Services Center.

8. I understand that the use of WiFi wireless capability on government issued/authorized tablets and laptops is only allowed in designated areas of USTRANSCOM facilities.

- I will turn off wireless capabilities or set to "Airplane Mode" (if available) on my government-issued commercial mobile devices (laptops, tablets, and cellular devices) prior to entering any USTRANSCOM building.

- I will only operate government-issued commercial mobile devices in wireless mode in authorized WiFi access areas. Wireless will be turned off when transporting devices to and from approved WiFi access areas. See USTCI 5200.07, for authorized WiFi access areas.

- I will not use any WiFi/wireless devices within 1 meter (in all directions) of any classified environment/equipment unless specifically authorized by the USTRANSCOM Authorizing Official.

- I will not bring personally owned wireless/cellular devices into prohibited areas. I will power such devices off when they are stored in approved temporary storage areas, unless otherwise notified/informed that they may be left on while stored. See USTCI 5200.07 for approved storage areas.

9. I will not attempt to access or process data exceeding the authorized information system classified level. I will not transfer data from a classified machine/device to a machine/device of lower classification without an approved written waiver, a two-person integrity check, and an automated classification check with the appropriate tool. I will contact USTRANSCOM Protection Services Center for guidance.

10. I will safeguard and mark with the appropriate classification level all information created, copied, stored, or disseminated from the information system and will not disseminate it to anyone without a specific need to know and appropriate clearance. I will back up all critical data to my network share or approved repository.

11. I will not alter, change, configure, or use operating systems, programs, or information systems except as specifically authorized. I will not introduce executable code (such as, but not limited to, .exe, .com, .dll, .vbs, or .bat files) without authorization, nor will I write or introduce malicious code.

12. I will not introduce unauthorized software to USTRANSCOM systems. I will submit a "New Capability" request through the "MyIT" service portal/JECC Internal Ticketing System or contact my Functional Area Communications Computer System Manager (FACCSM) for assistance.

13. I will not attempt to strain, test, circumvent, or bypass network or information system security mechanisms, or to engage in passive or active network discovery activities unless authorized and as part of my assigned duties.

14. I will not disclose or share my network access credentialing PINs. I will maintain personal custody of authentication tokens and common access cards (CACs) issued to me in accordance with Department of the Air Force Instruction 36-3026, Vol 1, "Identification Cards for Members of the Uniformed Services, Their Eligible Family Members, and Other Eligible Personnel." I will use my CAC to logon whenever possible. I will lock the computer or log off prior to leaving the computer and remove my CAC/SIPRNet token when the computer is not in use.

15. If I experience any IT issues or notice suspicious activity on my computer system or device, I will immediately contact the USTRANSCOM IT Service Desk/JECC Help Desk or my FACCSM.

16. I will contact the Command Foreign Disclosure Office (FDO) (618-817-7327), prior to releasing any information to a foreign user and appropriately mark all information cleared by the FDO.

17. I will report possible data spillage (Negligent Discharge of Classified Information [NDCI]), suspected information system tampering, or security incidents as soon as they happen or upon discovery to USTRANSCOM Cyber Operations Center (CyOC) (618-817-4222), the USTRANSCOM Protection Services Center, and my supervisor. For NDCI at JECC facilities, report to the JECC Information System Security Officer (ISSO).

_____	_____	_____
Name	Date	Signature

Instructions

1. **Initial:** Upon completion of initial cyber awareness training, review the contents of the form and complete. Provide the signed form to the supervisor or sponsor. The supervisor/sponsor will submit to the Directorate security manager for processing and forwarding to TCJ6-OM (USTRANSCOM facilities) or JECC ISSO.

2. **Annual:** Upon completion of annual cyber awareness training, review the contents of the form and complete. Provide the signed form to TCJ6-OM (USTRANSCOM facilities) or JECC ISSO.

Disposition Instructions

1. Form may be electronically transmitted, faxed, or mailed to TCJ6-OM.

2. Must be maintained on file for one year after termination of user's employment (permanent change of station, retirement, termination, etc.).

3. When no longer needed, destroy/delete file.