VISITING AEDC: REQUIREMENTS FOR U.S. TEST CUSTOMERS

All required actions and documentation will be completed/submitted ***at least 15 working days prior*** to the expected visit date. Failure to meet the submission date **will result in delays** at the Visitor Control Center (VCC) for badging, as well as computer account setups and access to test networks and internet service.

IMPORTANT POINTS OF CONTACT		
POC	**Phone**	**Email**
NAS Personnel Security (Visit Request)	931.454.5821 931.454.3474 (fax)	AEDC/Visit Requests
Customer Service Representative – CSR (Package Process Assistance)	931.454.6641 931.454.5426 931.454.5026 (fax)	AEDC/Test Customer Service
AEDC Visitor Center (Badge Request)	931.454.4010 931.454.4007 931.454.7937	AEDC Visitor Control Center

CHECKLIST: Depending on your specific requirements, you will be required to submit the following to the Customer Service Representative (CSR) and/or your AF Test Manager (TM) who can provide to the CSR:

1. **Visit Request and Badging Information**, as directed in this package, Enclosure #1.
2. **Completed Information System & Device Requirements**, **Sections 1-3**, Enclosure #2.
   a. Required if requesting access to government systems and/or to carry your organization's portable electronic device into a Classified test area; includes **laninfo.txt file (**which is required for connection).

   NOTE: Approval (completion of Enclosure #2) for unclassified customer computer equipment to be used in stand-alone mode and within a posted controlled unclassified area **is not required**. However, wireless capabilities mustbe **disabled** before introducing into a **posted controlled unclassified area**; test customers should receive guidance from their organization's ISSO/M on disabling. Devices will be subject to audit.
3. **Cyber Awareness Training Certificate**

   https://public.cyber.mil/training/cyber-awareness-challenge/
   a. Required if requesting access to government systems (annual requirement).
   b. Obtain a .pdf of the training certificate for submission to TM or CSR.
4. **Signed AF Form 4394**, *Air Force User Agreement Statement – Notice of Consent Provision,* Enclosure #3.
   a. Required if requesting access to government systems; print, sign, and date.
5. **Properly completed and signed System Access Authorization Request (SAAR)** for each government network for which access is required, Enclosure #4.
   1. Required if requesting access to government systems (one SAAR required per each, unique system).
   2. CSR or AF TM will provide appropriate SAAR (DD2875) templates, depending on requested systems.
   3. Please note that even if you are a returning customer and had previous access, a new SAAR is required.

6. **Information System Security Manager (ISSM) Certification of Wireless Removal,** Enclosure #5.
   a. Required if customer-owned computer equipment is to be introduced into classified areas.
   b. All wireless capability **must be removed** from customer-owned mobile computing equipment and the test customer's organization Information System Security Manager/Officer (ISSM/O) must certify in writing removal has occurred.

VISIT REQUESTS & BADGING INFORMATION, ENCLOSURE #1		
Type of Visit & Requirements	**Submit Request via DISS**	**Action Required**
Unclassified Visit with **No Access or Connectivity** to Government Networks or Computers, including Internet Connectivity and Stand-Alone	No**1, 2**	Submit the following information to the Customer Service Representative (CSR) for a badge request: Visitor Full Name Organization Facility to Visit Purpose of Visit Visit Start/End Dates Citizenship
Unclassified Visit with System Access or Connectivity to Unclassified Government Networks or Computers* *Minimum requirement for access is a T1 investigation.	Yes**1,2,3**	**Visitors without a DoD Security Clearance**: Submit a visit request, signed by organization's FSO, and via fax or encrypted e-mail to NAS FSO. Request must include: Visitor Full Name Organization AEDC Facility to Visit Purpose of Visit Visit Start/End Dates Citizenship Status Individual's T1 (NACI) Investigation Date*
Classified Visit	Yes**1,2,3**	**Visitors with a DoD Security Clearance**: Submit via DISS to National Aerospace Solutions (NAS),Cage Code **77SY44**. If DISS is not an option, visit request may also be sent via encrypted email or fax. **Visitors with a Clearance Equivalent to DoD Security Clearance** (i.e. NASA, DOE, etc.): Submit in their organization's prescribed format via encrypted e-mail or fax, signed by an appropriate clearance verification authority and will include visitor full name, organization & operating location, facility to visit, purpose of visit, visit start/ end dates, citizenship status, and security representative info (name, phone, e-mail address)

[1]An AEDC-issued badge is required for **all visitors** to AEDC, regardless of whether you already possess a CAC (active duty, retired DoD, or outside contractor issued).

[2]**REAL ID Requirements at AEDC**: If visiting personnel have driver's licenses that state "NOT FOR FEDERAL IDENTIFICATION" or "FEDERAL LIMITATIONS MAY APPLY," or if they are from a state that has implemented REAL ID and do not have a compliant driver's license, then they must also produce another form of ID at theVisitor Control Center (VCC), (along with the driver's license that is not REAL ID compliant), such as an unexpired U.S. Passport or Social Security Card (NON-LAMINATED).

[3]Customers who frequent AEDC, may submit a request up to one year in duration (1 Oct through 30 Sept).

VISITING AEDC: REQUIREMENTS FOR U.S. TEST CUSTOMERS

INFORMATION SYSTEM AND DEVICE REQUIREMENTS, SECTIONS 1-3, ENCLOSURE #2

SECTION 1. CUSTOMER INFORMATION

DATE:			
CITIZENSHIP:			
CUSTOMER NAME:	*LAST NAME*	*FIRST NAME*	*M.I.*
OFFICE SYMBOL/DEPARTMENT:		JOB TITLE:	
AEDC POCS/SPONSORS:			
COMPANY NAME:			
STREET ADDRESS:			
CITY, STATE, ZIP:			
CONTRACTORS ONLY—*CONTRACT NUMBER & EXPIRATION DATE:*			
BUSINESS TELEPHONE:			
OFFICIAL E-MAIL ADDRESS:			
MISSION REQUIREMENT/IMPACT:	*(DETAIL SPECIFIC IMPACT IF REQUIREMENTS CANNOT BE MET)*		

SECTION 2. REQUEST ACCESS

SENSITIVITY

Program classification: ❑ **CLASSIFIED** ❑ **UNCLASSIFIED**

ACCOUNT SETUP (CHECK ALL THAT APPLY)

❑ Account Login to test or other government networks (check all AEDC computer system(s) for which access is requested).

❑10V ❑ARGUS ❑ARTEMIS (HPC) ❑4T ❑VKF ❑16T ❑7V ❑12V ❑Mark I ❑STAT

❑CADDMAS: ❑C1 ❑C2 ❑J1 ❑J2 ❑J6 ❑SL2 ❑SL3

❑EDAPS: ❑C1 ❑C2 ❑J1 ❑J2 ❑J6 ❑SL2 ❑SL3

❑Use your existing CAC on unclassified network.

❑Internet Access only, connecting your organization's laptop to AEDC network.

❑Virtual Private Network configuration. Due to potential firewall process change requests, the following information is needed ***at least 15 working days in advance of visit.*** Ensure the Internet Protocol Address and Port Protocol Service is included in Section 3; seek assistance from your organization's Information System Security Manager/Officer (ISSM/O), if needed.

OTHER REQUIREMENTS (CHECK ALL THAT APPLY)

❑Connect your organization's computer equipment to AEDC's test networks for data acquisition and analysis purposes; **personally owned devices are prohibited for connectivity**.

❑Use your company's laptop or other portable electronic device (PED) (regardless of connectivity requirements) in classified area.

Section 3. LAPTOP AND/OR OTHER PORTABLE ELECTRONIC DEVICE (PED) IDENTIFICATION (*laninfo .txt file required; refer to information*, below),* Enclosure #2

Item	Classification	For Internet Use Only (Y/N)?	Connect to Test Network (Y/N)?	Manufacturer	Dates of Use	Model No.	Serial No.	List Capabilities (wireless, GPS, camera, video, etc.)	Wireless MAC Address	Wired MAC Address	VPN Configuration Required (Y/N)?*	Provided Internet Protocol Address	Provide Port/Protocol Service	Use Existing CAC on AEDC Network (Y/N)?
Laptop	Unclassified	Y	N	Hewlett Packard	12/3/2015 to 12/15/2015	EX: HP1234	EX: 8K12345678	Wireless, GPS, camera, video						N

*The following must be properly configured on your portable device by your organization's Information System Security Manger/Officer (ISSM/O) **prior to your arrival**. For Internet Connectivity, AEDC requirements are:

1. Active Ethernet port.
2. Standard straight through Cat5e/Cat6 network cable of reasonable length (6 foot or greater) terminated with RJ-45 connectors.
3. Configured for auto negotiation for speed and duplex.
4. Configured for Dynamic Host Configuration Protocol (DHCP) for both IP addressing and Domain Name Service (DNS).

Generate the laninfo.txt file, as follows:

1. Ensure wired LAN interface is enabled
2. Open a command window: ->START ->Run ->Type "CMD" and press "Enter"
3. At command prompt in command window, type **ipconfig/all>>laninfo.txt** and press "Enter"
4. Text fill will be generated to area where indicated by C: prompt in command screen (i.e. C:\DocumentsandSetting\YOUR-NAME).
5. Include the laninfo.txt with this completed form (Information System & Device Requirements, Sections 1-3).

AIR FORCE USER AGREEMENT STATEMENT - NOTICE AND CONSENT PROVISION

By signing this document, you acknowledge and consent that when you access Department of Defense (DoD) information systems:

You are accessing a U.S. Government (USG) information system (IS) (which includes any device attached to this information system) that is provided for U.S. Government-authorized use only.

You consent to the following conditions:

The U.S. Government routinely intercepts and monitors communications on this information system for purposes including, but not limited to, penetration testing, communications security (COMSEC) monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations. At any time, the U.S. Government may inspect and seize data stored on this information system.

Communications using, or data stored on, this information system are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any U.S. Government-authorized purpose.

This information system includes security measures (e.g., authentication and access controls) to protect U.S. Government interests -- not for your personal benefit or privacy.

Notwithstanding the above, using an information system does not constitute consent to personnel misconduct, law enforcement, or counterintelligence investigative searching or monitoring of the content of privileged communications or data (including work product) that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Under these circumstances, such communications and work product are private and confidential, as further explained below:

Nothing in this User Agreement shall be interpreted to limit the user's consent to, or in any other way restrict or affect, any U.S. Government actions for purposes of network administration, operation, protection, or defense, or for communications security. This includes all communications and data on an information system, regardless of any applicable privilege or confidentiality.

The user consents to interception/capture and seizure of ALL communications and data for any authorized purpose (including personnel misconduct, law enforcement, or counterintelligence investigation). However, consent to interception/capture or seizure of communications and data is not consent to the use of privileged communications or data for personnel misconduct, law enforcement, or counterintelligence investigation against any party and does not negate any applicable privilege or confidentiality that otherwise applies.

Whether any particular communication or data qualifies for the protection of a privilege, or is covered by a duty of confidentiality, is determined in accordance with established legal standards and DoD policy. Users are strongly encouraged to seek personal legal counsel on such matters prior to using an information system if the user intends to rely on the protections of a privilege or confidentiality.

Users should take reasonable steps to identify such communications or data that the user asserts are protected by any such privilege or confidentiality. However, the user's identification or assertion of a privilege or confidentiality is not sufficient to create such protection where none exists under established legal standards and DoD policy.

A user's failure to take reasonable steps to identify such communications or data as privileged or confidential does not waive the privilege or confidentiality if such protections otherwise exist under established legal standards and DoD policy. However, in such cases the U.S. Government is authorized to take reasonable actions to identify such communication or data as being subject to a privilege or confidentiality, and such actions do not negate any applicable privilege or confidentiality.

These conditions preserve the confidentiality of the communication or data, and the legal protections regarding the use and disclosure of privileged information, and thus such communications and data are private and confidential. Further, the U.S. Government shall take all reasonable measures to protect the content of captured/seized privileged communications and data to ensure they are appropriately protected.

In cases when the user has consented to content searching or monitoring of communications or data for personnel misconduct, law enforcement, or counterintelligence investigative searching, (i.e., for all communications and data other than privileged communications or data that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants), the U.S. Government may, solely at its discretion and in accordance with DoD policy, elect to apply a privilege or other restriction on the U.S. Government's otherwise-authorized use or disclosure of such information.

All of the above conditions apply regardless of whether the access or use of an information system includes the display of a Notice and Consent Banner ("banner"). When a banner is used, the banner functions to remind the user of the conditions that are set forth in this User Agreement, regardless of whether the banner describes these conditions in full detail or provides a summary of such conditions, and regardless of whether the banner expressly references this User Agreement.

1. NAME (Last, First, Middle	2. STATUS ☐ Military ☐ Civilian ☐ Contractor
3. USER SIGNATURE	4. DATE (YYYYMMDD)

AF FORM 4394, 20130621

AUTHORITY: 10 U.S.C. Section 8013: Secretary ofthe AW- Force. AFI 33-332: and E.O. 9397 {SSN)

ROUTINE USE: None.
DISCLOSURE IS VOLUNTARY: Failure to provide the SSN would make it difficult to identify you and your records when the user agreement is processed and filed. SSN is not required f« contractors.

INSTRUCTIONS FOR COMPLETING SYSTEM ACCESS AUTHORIZATION REQUEST (SAAR) – DD2875, Enclosure #4

A SAAR or DD2875 is required for each unique government network for which access is requested. Please contact your AF TM or CSR for appropriate templates, if needed. Failure to complete the DD2875 properly, as directed below, results in delays.

These are the only fields that require completion:

TYPE OF REQUEST: Click "Initial" (regardless of whether you've had an account on the system in the past; accounts are disabled after test program completion.

USER ID: If you possess a CAC card, enter the DoD ID Number from the back of the card; otherwise, leave blank.

DATE: Self-Explanatory

SYSTEM NAME: The name of the system will already be entered in the DD2875 template(s) provided to you by the CSR or AF TM; no entry is required by the customer.

LOCATION: Arnold AFB, TN

PART I

Blocks 1-10: Self-Explanatory.

Skip to Block 13, saving Blocks 12 and 11 for last.

PART II

Block 13: "Required to support Test Program XXXXX."

Block 14. Select "Authorized"

Block 15. Select appropriate classification of system.

Block 16a. Enter the Contract # and Expiration Date associated with the test program to be conducted at AEDC.

Block 27. The options in this block vary, depending on which DD2875 template/system is used; if needed, request guidance from AF TM or CSR.

Block 12: Enter date.

Block 11: Digitally sign.

CERTIFICATION OF WIRELESS CAPABILITY REMOVAL FOR DEVICES INTRODUCED TO CLASSIFIED AREAS, Enclosure #5

To: NAS Industrial Security / Information Systems Security Manager (ISSM)

From:

Date Certified:

I certify that all wireless capability has been removed from the following devices and camera lens (if applicable) have been covered with metallic tape:

Item Description	Model #	Serial #

Certifying Official Signature/Organization/Title (ISSM or IA Level II Personnel required)

FREQUENTLY ASKED QUESTIONS (FAQS)

What do I need to know about information system or electronic device usage at AEDC?

1. DoD computer usage at AEDC is monitored.
2. DoD **prohibits** use of any flash memory device, music disks or other unofficial media in DoD computers, equipment, or networks/standalones or in systems connected to DoD computers, equipment, or networks.
3. Do not attempt to access, connect to, or place devices or media in a DoD computer or network, including standalone systems unless authorized to do so.
4. Wireless devices, air cards, recording and/or photographic devices, including cell phones, are prohibited in certain areas to include **controlled unclassified areas**; adhere to an area's posted signage that state the restrictions.
5. Do not remove or release AEDC equipment, software, media, or information without proper approval.
6. Hardware, software, and media must be clearly marked upon creation with the classification level. Military data requires a DoD distribution statement, export control warning and destruction notices per sponsoring agency.
7. Hard drives connecting to AEDC computers will be provided by AEDC. Customer-provided hard drives will NOT be used.
8. Personal medical devices with Bluetooth/wireless capabilities must be coordinated in advance with NAS Industrial Security.

What about using my personally owned electronic devices at AEDC?

1. Personal cell phones can be used, but only as a telephone, in non-posted areas (hands-free mode when operating a vehicle).
2. Do **NOT** use a cell phone, or any other unauthorized device to take pictures or videos while at AEDC (NOTE: Identify photography requirements to your AEDC host, who will ensure authorized equipment is provided and processes are followed).
3. Personally owned electronic devices or media are not authorized in posted areas, even if it is an unclassified area.
4. Do **NOT** synchronize or connect personally owned electronic devices (even for battery charging) to DoD computers, equipment, or networks, including standalone DoD laptops.
5. Do **NOT** introduce government-owned information to a personally owned device, including taking photographs with a cell phone while at AEDC.

GENERAL GUIDANCE FOR VISITORS

1. Do not use prohibited devices within posted areas without written approval.
2. Do not attempt to enter work or service areas unless you are authorized to be there.
3. Properly dispose of sensitive information in locked shred bins or return to your AEDC visit sponsor.
4. Always wear AEDC badge properly (above the waist, outside outer most layer of clothing); do not alter, deface, or destroy a badge; do not misuse a badge (i.e., lending to another individual or using for identification purposes away from AEDC).
5. Observe traffic, parking rules and requirements.
6. Obey speed limits. Unless otherwise posted, AEDC speed limit is 35 mph; 20 mph at gates; 15 mph in parking lots. Pedestrians have right-of-way.

7. Seat belt use is required.
8. Dual citizenship visitors must disclose dual citizenship and must provide proof of U.S. citizenship (U.S. passport or naturalization paper).
9. Vehicles are subject to random search upon entry and exit; registration and proof of insurance are required.
10. Do not introduce, transport, use or possess ammunition, firearms, explosives, or other lethalweapons in the AEDC fenced mission area.
11. Do not disregard safety rules and common safety practices.
12. Do not use tobacco products and/or "strike" matches when or where prohibited.
13. Do not possess or use intoxicants, narcotics, or illegal controlled substances on AEDC.
14. Alcohol is prohibited within fenced mission area. **EXCEPTION:** when purchased at the Base Exchange, unopened within original wrapper/container, and accompanied with a sales receipt.

All Emergencies at AEDC (Fire/Ambulance/Police) can be reported by dialing **9-1-1**. Inform the operator you are calling from AEDC.