Arnold Air Force Base U.S. AIR FORCE

Visiting Arnold Engineering Development Complex (AEDC) *www.arnold.af.mil*

April 2016

U.S. Citizenship

This information is for visiting test customers who are **U.S. citizens that work for a U.S.-owned company.** If you are a Lawful Permanent Resident (LPR), have dual citizenship, or are a U.S. citizen who works for or is conducting work for a foreign-owned company, visit requirements are different. Advise your AEDC POC who will provide further guidance.

Important Points-of-Contact

In addition to your specific T&E points-of-contact, the following can assist with meeting your requirements to visit AEDC:

	Responsible for	**Telephone**	**Fax**	**eMail**
Personnel Security	Visit Authorization Letter (VAL) / Clearance and Investigation Validation for classified test programs/visits or unclassified test programs/visits with computer access.	931-454-6003 931-454-5680	931-454-3474	Vivian Seals Mary Beth Barlow
Customer Service for Test Areas	Customer Service Representatives (CSR) *Liaison between Security, Information Assurance, AEDC Project Managers/Test Engineers, and Customers to meet customers' visit requirements, including computer access.* ***Customers should contact CSR for assistance.*	931-454-6641	931-454-5026	Sylvia Armer
	CSR Alternates	931-454-7873	931-454-4611	Alecia Davis
AEDC Visitor Center	Issue AEDC badges after investigation verification.	931-454-4010 931-454-4007 931-454-7937	--	--

Base Access

Requirements for AEDC

1. Visitor Badge, **and**
2. DoD Common Access Card (CAC) or locally-prepared equivalent for non-DoD personnel

Arriving at AEDC

1. Stop at the Visitor Center (VC) outside the Main Gate.
2. Present your DoD CAC, or other positive form of identification in lieu of the DoD CAC.
3. VC will issue a visitor badge and a locally-prepared equivalent to a DoD CAC if you do not have the latter.

Main Gate

1. Present both your visitor badge and DoD CAC or locally-prepared equivalent, whichever of the latter is applicable.
2. Always wear your visitor badge while at AEDC.
3. A valid driver's license, proof of insurance and registration (or rental agreement) is required for your vehicle.

Badge Retention

1. Until it expires, or until no longer required (even though it is still valid)
2. Surrender badge by dropping into the box or handing to Police at the Main Gate as you are leaving AEDC.

Visit Request

A request may be required for your visit to AEDC; please review the following table to determine your requirements. Customers who frequent AEDC often may submit a request to span an FY (1 October through 30 September). Allow **10** working days for processing a visit request.

Type of Visit(or) & Computer/Network Requirements	**Submit VAL?**	**How to Submit Visit Request**
Unclassified Visit – No access or connectivity to government networks/ computers (including internet) required	No	Visit Request Not required **IMPORTANT:** An AEDC badge is required regardless of whether you are required to submit a visit request. Submit **visitor name, organization, facility to visit, purpose of visit, visit start/end dates, and citizenship status** to the respective area's Customer Service Representative (CSR) – identified above under "Important Points of Contact."
Unclassified Visit – access or connectivity* to government networks/ computers (including internet) requested **or** **Classified Visit** with connectivity* or without connectivity	Yes Yes Yes	Visitors with a DoD security clearance submit via Joint Personnel Adjudication System (JPAS) to Akima Support Operations (ASO) Cage Code 5U5K84 with "**ARNOLD AFB** in the **ORGANIZATION LINE** of the **VAL**"; visit requests may also be sent via **encrypted** email, or fax, but JPAS is the preferred method. Visitors without a DoD security clearance submit FSO-signed VAL via fax or **encrypted** email to ASO FSO and include: • Visitor Full Name, Organization, Facility to Visit, Purpose of Visit, Visit Start and End Date, Citizenship • Individual's National Agency Check with Inquiries (NACI) date, as well as the organization that performed the background investigation. Visitors with a clearance equivalent to DoD security clearance (i.e., NASA, DOE, etc.) submit via their organization's prescribed format via **encrypted** email or fax, but must include Visitor Full Name & Citizenship, Organization & Operating Location, Facility to Visit, Purpose of Visit, Visit Start and End Date, Citizenship; and Security Representative Name, Phone, eMail address.
***Complete Information System Requirements Questionnaire U.S Test Customers (pages 6 & 7)**		

Information Protection (IP)

1. Customers will not be allowed to work in contractor-controlled unclassified or classified areas unless authorized personnel are present; these areas include buildings (after-hours / weekend entry), control rooms or any other data processing areas, high bays, or buildup areas, and test cells or wind tunnels.
    a. If a Customer Room has been designated for a program, customers may work in that area alone as long as authorized personnel are present in the building.
    b. Customers may be provided an entry code or PIN swipe to certain areas; codes must be protected at the same level as the program and cannot be divulged.
    c. Customers must not allow "tailgating" into an area that is controlled by an entry code or PIN swipe unless they are positive the other individuals should come into the area.
2. Customers cannot use or introduce prohibited devices (flash memory devices such as thumb, jump, and flash drives, as well as music disks or other unofficial media) into contractor-controlled unclassified or classified areas.
3. Customers should observe and adhere to the posted signage in AEDC's facilities regarding use of electronic devices.
4. Customers cannot extend invitations for visits to AEDC; only authorized AEDC personnel can sponsor a visitor.
5. Customers cannot release AEDC information (including photographs, videos, etc.) without proper coordination and authorization with the AEDC project managers and Industrial Security.

Information Assurance (IA)

Frequently Asked Questions (FAQs)

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

1. Department of Defense (DoD) computer usage at AEDC is monitored.
2. DoD **prohibits** use of any flash memory device (thumb, jump, and flash drives, camera cards), as well as 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 you have been authorized to do so.
4. Wireless devices, air cards, recording and/or photographic devices, including cell phones, are prohibited in certain areas; adhere to an area's posted signage that states 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. **PLEASE NOTE: AEDC does not provide long-distance calling service for customers; customers should bring a phone card if using AEDC phone system for long-distance.**

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.

What if I want to use my company-owned laptop or device as a stand-alone for official use?

1. A company-owned laptop/electronic device with **no connectivity requirements** may be introduced for official use into **posted unclassified** areas without authorization from ASO Facility Security Officer (FSO) or ATA Information Assurance Manager (IAM):
   a. Must disable wireless capability and ensure it remains disabled unless in areas approved for public wireless access.
      - Small dark red plastic window on the laptop indicate infrared capability; this window **must** be completely covered with metallic tape.

   b. Must remove camera/video and/or GPS locator technology software programs.

What if I want to connect my company-owned laptop to a DoD network or stand-alone, if I want to use a DoD system, or if I want to use my PED in a classified area?

1. You **must complete and submit to the Customer Service Representative (CSR), at least 10 working days prior to your planned arrival**:
   a. Visit request via JPAS (or as otherwise directed on page 1).
   b. Complete “Information System Requirements Questionnaire.
   c. DoD IAA CyberAwareness Challenge certificate (see “**IA Training**,” below).

IA Training

Personnel granted access to U.S. government information systems must complete initial (and thereafter annually) CyberAwareness training. This training educates users on the basic principles of network security and their roles and responsibilities for IA (Refs: AFI 33-200, para 2.27.6; AFSSI 8522, para 3.1.1).

A Common Access Card (CAC) is not required to access or complete this training; it is available online at: http://iase.disa.mil/.

1. Under Cybersecurity Training column on right side, click on “Education, Training and Awareness (ETA).”
2. Towards the middle of the page you will see a group of selection under the heading Top Online Trainings! click on “Cyber Awareness Challenge, Version 3.0, December 2015**.”**
3. Click on “Launch New Cyber Awareness Challenge Department of Defense Version” to launch the course.
4. At the end of the course, follow the instructions to obtain and print a certificate (**a certificate must be printed and submitted as directed or credit will not be given and the test will have to be retaken**).

Test customer information systems are also subject to IA requirements. These systems are identified, and specific guidance provided, either in a DoD Service Level Agreement and/or the Test Security Plan.

> **NOTE**: Computers whose functions include test article control, etc., and that are an inherent part of the article/article’s operation are excluded from IA requirements.

Safety

1. **If you require access to an AEDC Industrial Area’s Confined Space and/or Control of Hazardous Energy, you must complete the attached Safety Questionnaire (see Page 10)**.
2. The following is general guidance only and **specific safety requirements for your visit should be discussed with your AEDC POCs**.
3. Personal Protective Equipment (PPE) is required in all industrial and construction areas
   a. Minimum hard hat, safety shoes and safety glasses (prescription safety glasses with side shields if you wear glasses).
   b. Your AEDC POC can provide hard hats and non-prescription safety glasses.
4. Comply with OSHA and AEDC Safety, Health & Environmental Standards, including but not limited to Confined Space Entry, Lockout/Tagout, Master Work Permits, Flame Permits, etc.
5. Obey all postings and audible alarms.
6. Do not cross barricades unless specifically authorized to do so.
7. Know where to go in the event of a severe weather warning. AEDC issues a warning when lightning is within 10 miles of the base.
8. Do not operate machinery or other devices unless qualified and authorized.

9. Smoke only in approved, designated areas.
10. Report all injuries to your AEDC POC.

Emergency Contact Numbers

1. All emergencies at AEDC (Fire/Ambulance/Police) can be reported by dialing 9-1-1. State the nature of emergency and stay on the line until told to hang up.

All Emergencies	911
Fire	454-5648
Arnold Protective Services	454-5662
Operations Center	454-7752
Safety	454-7233
Radiation Safety	454-5446

   a. If calling 911 from personal cell phone, inform operator you are calling from Arnold Air Force Base (not necessary if you're calling from a Base phone). Stay on the line until told to hang up

2. Report:
   a. Any condition, practice or situation that poses a hazard
   b. Accidents (personal or vehicle) or injuries
   c. Fire/Explosion, Spills or Near-Misses
3. Be aware of evacuation routes posted in each building.
4. If fire or other alarms are activated, vacate in an orderly fashion and do not use elevators.

Hazardous Materials

1. Inform your POC if you plan to bring any hazardous material to AEDC.
2. Such materials require Safety Data Sheets (SDS) and documentation of HazCom training prior to use.
3. Radioactive materials or radiation producing devices must be approved by the Installation Radiation Safety Officer (IRSO) BEFORE they are brought on-base.
4. Ensure that required HazCom information is available at the job site.

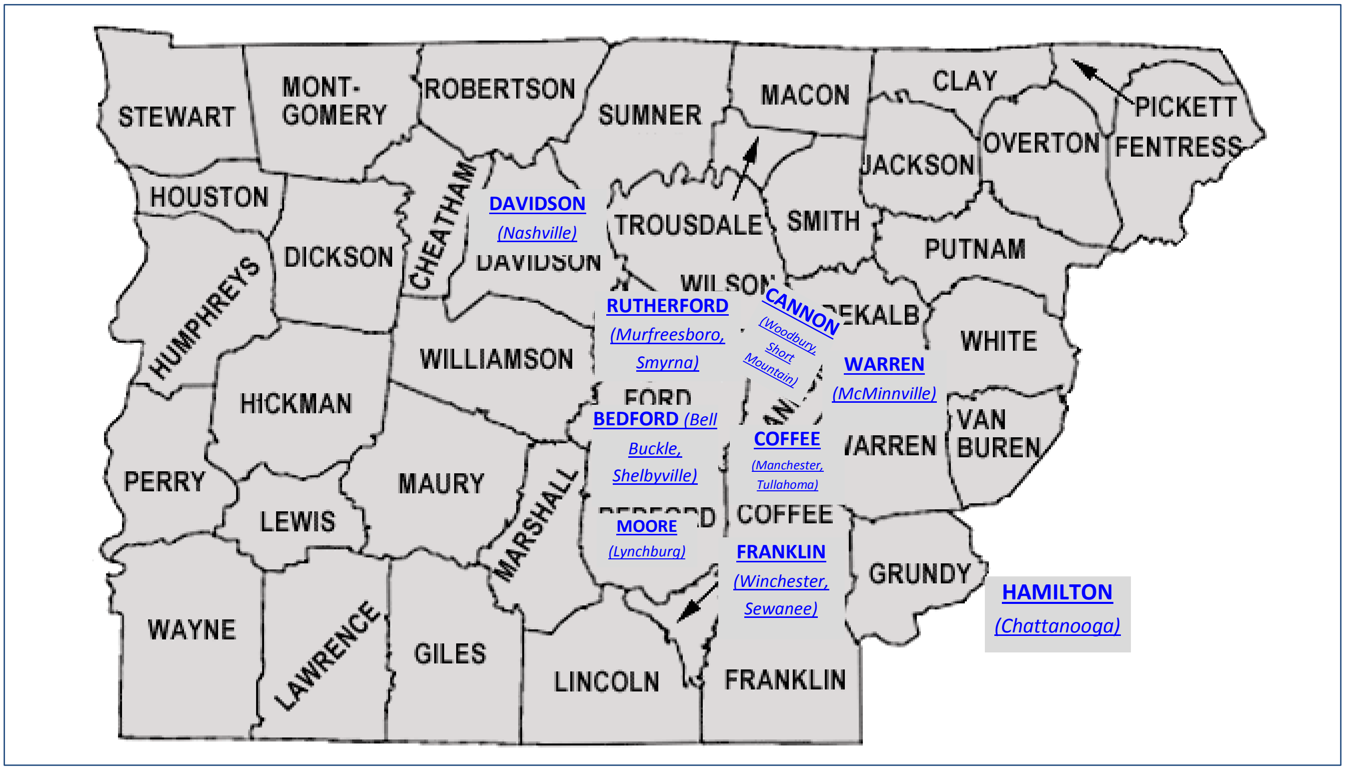
Environmental

1. Do not litter; recycle where possible.
2. Do not pour hazardous (or suspected hazardous) materials into drains, sewers, lakes or streams.
3. If you should accidentally spill something hazardous (or suspected hazardous), please report it immediately.

General Base Security

1. Do not use prohibited devices within posted areas without the written approval of the ASO Facility Security Officer (FSO) or the Chief, AF Information Protection Office (AEDC/TSD-IP). Refer to Section "Information Assurance."
2. Do not attempt to enter work or service areas unless you are authorized to be there.
3. Properly dispose of sensitive information in the locked shred bins or return to your AEDC visit sponsor.
4. Always wear your AEDC badge properly; 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. Seat belt use is required.
6. Observe traffic, parking rules and requirements. Obey speed limits. Unless otherwise posted, the AEDC speed limit is 35 mph; 20 mph at gates; and 15 mph in parking lots. Pedestrians have right-of-way.
   a. There are additional requirements for motorcycles; if you need those requirements, notify your AEDC POC.
7. Vehicles are subject to random search upon entry; registration and proof of insurance are required.
8. Do not introduce, transport, use or possess ammunition, firearms, explosives, or other lethal weapons in the AEDC fenced mission area, including even within a vehicle.
9. Do not disregard safety rules and common safety practices.
10. Do not use tobacco products and/or "strike anywhere" matches where or when prohibited.
11. Do not possess or use intoxicants, narcotics, or illegal controlled substances on AEDC.
12. Alcohol is prohibited within the fenced mission area. **EXCEPTION:** Alcohol is allowed when purchased at the Base Exchange, unopened within its original wrapper/container, and accompanied with a sales receipt.

Middle Tennessee Information



Driving Directions, Area Maps

Wingo Inn

Information System Requirements Questionnaire: U.S. Test Customers

Section 1. Customer Information

Date:			
Citizenship:			
Customer Name:	***Last Name***	***First Name***	***MI***
Office Symbol/Department		*Job Title:*	
AEDC POCs/Sponsors:			
Company Name:			
Street Address:			
City, State, Zip:			
Contractors ONLY--*Contract Number & Expiration Date:*			
Business Telephone:			
Official eMail Address:			
Mission Requirement/Impact	*(Detail specific impact if requirements cannot be met).*		

THIS FORM IS FOR OFFICIAL USE ONLY (FOUO) WHEN COMPLETED / PROTECT ACCORDINGLY

Section 2. Request Access

1. What are your requirements (check all that apply):

   Is the test ☐ classified or ☐ unclassified?

   ☐ 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 ☐Other (specify):

   ☐ Connect your organization's laptop (or other portable electronic device, PED) to AEDC network for Internet access; **personally-owned devices are prohibited for connectivity**.

   ☐ Virtual Private Network configuration. Provide this information two weeks in advance if you are a new customer for AEDC or you have not been a customer for more than one year, to allow for sufficient time to process firewall change requests. For assistance with completing the following, please contact the Information Assurance (IA) Office at 931-454-3941 or 931-454-3871.
   Internet Protocol Address (provide if VPN configuration selected) – the IP address of the VPN device at your company to which you will be connecting while at AEDC:
   Port Protocol Service (provide if VPN configuration selected) – the transmission mechanism for connecting to the endpoint site; common ports are 443, 4500, 500, etc.:

   ☐ 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 existing CAC on AEDC network/system

   ☐ Use your company's laptop or other portable electronic device (PED) in classified area

Section 3. Specific Requirements

PLEASE NOTE: PERSONALLY-OWNED LAPTOPS OR PORTABLE ELECTRONICS DEVICES ARE NOT APPROVED FOR CONNECTION TO AEDC SYSTEMS/NETWORKS

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)?*	Provide 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: HPZ420	EX: 8XK4839109	Wireless, GPS, camera, video			N	N/A	N/A	N
												y		

*For VPN configuration, provide information 2 weeks in advance if you are a new customer for AEDC or you have not been a customer for more than one year to allow for sufficient time to process firewall change requests. For assistance with completing the required information, contact the Information Assurance Manager, Scott Williams, 931-454-4105.

**The IP address of the VPN device of your company to which you will be connecting while at AEDC.

***The transmission mechanism for connecting to the endpoint site; common ports are 443, 4500, 500, etc.

GENERAL INFORMATION ABOUT CONNECTIVITY AT AEDC & BASIC STEPS FOR FINDING/DOCUMENTING WIRED & WIRELESS MAC ADDRESSES

PASSWORDS

1. Passwords for computers that connect to any AEDC resource must:
   a. Be fifteen (15) characters (2 upper case, 2 lower case, 2 numbers and 2 special characters (@&+!, etc).
   b. Be changed every sixty (60) days.
   c. **Not** be written down.
2. **Use password-protected** screen savers and **immediately** activate whenever computers are left unattended.

NETWORK - Please inform your IT department of these requirements so they can configure your device appropriately.

Internet Connectivity

- IA requires your Media Access Control (MAC) address for your device(s) wireless interfaces when you complete **Section 3. Information Systems Requirement Questionnaire; locate address by doing the following:**
  1. Ensure your wired LAN interface is enabled.
  2. Open a command window: -> START -> Run -> Type "CMD" and press Enter
  3. At the command prompt in command window, type **ipconfig /all >> laninfo.txt** and press "Enter"
  4. Text file will be generated to area where indicated by C: prompt in command screen (i.e., C:\Documents and Setting\YOUR-NAME)
  5. Include the generated .txt file with **Information Systems Requirement Questionnaire.**
- Active Ethernet port
- Standard straight through Cat5e/Cat6 network cable of reasonable length (6 feet or greater) terminated with RJ-45 connectors
- Configured for auto negotiation for speed and duplex
- Configured for Dynamic Host Configuration Protocol (DHCP) for both IP addressing and Domain Name Service (DNS).

WIRELESS

- Operation of any sort of wireless communication technology associated with customer-owned computing equipment is prohibited in all AEDC test areas.
- Test customers are required to disable all such wireless interfaces and ensure they remain disabled unless in areas approved for public wireless access.
- Identifying wireless capabilities:

✓ A Wi-Fi or Bluetooth logo sticker on the laptop indicates it **has** built-in wireless networking capabilities.

✓ A wireless network connection icon indicates that the laptop supports wireless networking.

✓ 802.11 can either be mini-PCIs located beneath a removable panel on the laptop's underside or external cards that plug into PCMCIA, Compact Flash, Secure Digital, Ethernet, or USB interfaces. **These external cards must be physically removed while in classified spaces.**

✓ Small dark red plastic windows on the laptop indicate infrared capabilities. These windows **must** be completely covered with metallic tape.

✓ Although not a wireless issue, laptops with camera/video and/or GPS locator technology installed must have the software program(s) uninstalled.

To disable wireless check with your local IT support staff prior to visit.

VIRUS & INCIDENT CHECKLIST

QUICK-REFERENCE

Virus Detected

✓ Do NOT turn off your computer!

✓ Do not delete the message or file.

✓ Do not forward infected email/document.

✓ Notify your IAM or immediate supervisor.

✓ IAM contact AEDC's Network Control Center (NCC) at 931-454-4040 and identify if the virus was downloaded from a document.

✓ Write down any errors that you observed on your system.

✓ Mark the computer "**DO NOT USE**."

Classified Spill Incident

✓ Do NOT turn off your computer!

✓ Do not delete the message/file.

✓ Do not forward relevant email.

✓ **Immediately** notify, in person or via **secure** phone, your IAM.

✓ **Immediately** notify AEDC's NCC at 454-4040 and follow instructions.

✓ Mark the computer "**DO NOT USE**."

✓ Ensure someone with appropriate clearance level physically guards the machine or secure the device in a classified area approved for same classification level.

Safety Training Questionnaire: U.S. Test Customers

Program Name:	
AEDC Facility:	
AEDC POCs:	

Employee Name	**Permit-Required Confined Space (PRCS)** **Most Recent Training Date**	**Control of Hazardous Energy (Lockout/Tagout)** **Most Recent Training Date**

Provide the above information, as well as certificates, letters, etc. (proof) of training to T&E Customer Service Reps.

Visit Checklist

1. Visit request submitted via JPAS (or as otherwise directed in this package, see page 1) for classified visits and/or if requiring connectivity to AEDC networks (regardless of visit classification).

2. Information System Requirements Questionnaire (pages 6-7) completed fully and correctly.

    a. Contractors ONLY: As part of the Questionnaire, the contract number and expiration date must be completed on this form; UNLESS it would render the form classified – leave blank in that instance.

3. Information Assurance Training Certificate current (good for one year).

4. Submitted Items #2-#4 to Customer Service Representative (refer to page 1).