

## **AEDC Customer Requirements for Using AEDC Computers & Internet Access**

To gain access to AEDC networks, including internet, individuals must be properly vetted by either a Security Clearance or a National Agency Check with Inquiries (NACI). If individuals do not possess these credentials, they must contact their security office to take appropriate action. If your company is not a cleared facility, contact the ATA Industrial Security Office for assistance (931-454-6003, DSN 340-6003).

When the requirements above have been met, complete the following prior to visit:

- Signed Customer Information and Compliance Signature Page
- Completed Information Assurance Awareness Training Test or current DoD Information Awareness certificate
- Completed U.S. Visitor/Customer *Request to Connect Company-Owned* Portable Electronic Device (PED) to AEDC Computer Systems/Networks and Internet Access if bringing company laptop to AEDC
- Test Customer Requesting VPN Access page two weeks prior to needing access
- A Visit Authorization Letter (VAL), which is accomplished by your Security Department, should be sent to ATA Industrial Security (Fax No. (931) 454-3474 or DSN 340-3474).

This document contains the following information for gaining access to AEDC Computers and Internet.

1. FY2010 DoD Information Assurance Awareness Training
2. Virus and Incident Checklist
3. AEDC Customer Information Assurance Briefing
4. Customer Information and Compliance Signature Page
5. U.S. Visitor/Customer *Request to Connect Company-Owned* Portable Electronic Device (PED) to AEDC Computer Systems/Networks and Internet Access
6. General Information about Connectivity at AEDC and Basic Steps for Finding and Documenting Wired and Wireless MAC Addresses
6. Test Customers Requesting VPN Access at AEDC

# FY2010 DoD Information Assurance Awareness Training

- ~ *Over 9 million Americans are victims of identity theft each year.*
- ~ *Security breach compromises over 20,000 government social security numbers.*
- ~ *17 People per minute have their identities stolen.*
- ~ *Who's protecting your social security number?*

## 1. Information Assurance (IA)

- The goals of IA are to protect our information and information systems. Information assurance is defined as, "Protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats."

## 2. Secure Information System

- A secure information system maintains the principles of confidentiality, integrity, availability, authentication, and non-repudiation.
  - **Confidentiality** safeguards information from being accessed by an individual without the proper clearance, access level, and need to know.
  - **Integrity** results from the protection of unauthorized modification or destruction of information.
  - **Availability** means that information services are accessible when they are needed.
  - **Authentication** is a security measure that establishes the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.
  - **Non-repudiation** means assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data.
- As an authorized user, you are also responsible for contributing to the security of all Government-owned computer systems. You must abide by these principles of IA in your daily work routine to protect Government-owned information and information systems.

## 3. Why is IA important?

- In the past, computers were standalone systems that were relatively easy to protect. What was once a collection of separate systems is now best understood as a single, globally connected network because of the interconnected nature of our information systems, a risk to one is a risk to all!

#### **4. Data Classification**

- Information, as well as our information systems, must be protected by IA. The DoD has two broad categories: classified and unclassified.
  - Classified information is designated as Confidential, Secret, or Top Secret. The specific level of classification assigned to information is determined by the original classification authority. Classified information must be used in an area that has been approved and cleared for the appropriate classification level. When not in use, classified information must be stored in a General Services Administration, or GSA, approved vault or container.
  - All DoD information, combined with the right conditions and circumstances, could provide an adversary insight into our capabilities and intentions. Additionally, the aggregation of unclassified information can elevate the sensitivity level of information. Therefore, even unclassified information, if compromised, could impact the safety of DoD personnel, missions, and systems. All DoD unclassified information not specifically cleared for public release requires some level of security protections. At a minimum, it must be reviewed before it is released, in any form, outside the U.S. government. For Official Use Only, or FOUO, and Controlled Unclassified Information, or CUI, can include, but is not limited to, personnel, financial, payroll, medical, operational, and Privacy Act information. FOUO and CUI must be stored in a locked drawer or secure container. When it is no longer needed, it should be destroyed.

#### **5. Critical Infrastructure Protection**

- If information and information systems are compromised, it can impact our way of life, our country's infrastructure, our national security, and, ultimately, cause the loss of lives. Critical infrastructure refers to the physical and cyber-based systems essential to the minimum operations of the economy and Government. U.S. sectors that are considered part of this infrastructure include, but are not limited to, information technology and telecommunications, energy, banking and finance, transportation and border security, water and emergency services. Critical Infrastructure Protection, or CIP, is a national program established to protect these critical infrastructures.

#### **6. Threats and Vulnerabilities**

- What exactly are we protecting Government-owned information and information systems from? Threats and vulnerabilities.
  - A threat is any circumstance or event that can potentially harm an information system by destroying it, disclosing the information stored on the system, adversely modifying data, or making the system unavailable.

Vulnerability is a weakness in an information system or its components that could be exploited. Vulnerabilities exist when there is a flaw or weakness in hardware or software that could be exploited by hackers. Vulnerabilities are frequently the result of a flaw in the coding of software.

## 7. Threat Categories

- Environmental Threats
  - Natural environmental events include lightning, fires, hurricanes, tornadoes, or floods. These natural events pose threats to your system and information.
  - Another kind of environmental threat is a system event. A system's environment, including poor building wiring, insufficient cooling, or power outages can cause harm to information systems.
- Human threats can be generated from internal sources or from external sources.
  - The greatest threats to information systems are internal, from people who have working knowledge of, and access to, their organization's computer resources. An insider is any person who has legitimate physical, user, or administrative access to the computer system. Insiders can misuse or exploit weaknesses in the system. Other users, due to lack of attention, or lack of training and awareness, can also cause serious damage. Although there are security programs to prevent unauthorized access to information systems, and employees undergo background checks, certain life experiences can alter a person's normal behavior and cause them to act illegally or irresponsibly. Stress, divorce, financial problems, or frustrations with co-workers or the organization are some examples of what might turn a trusted user into an insider threat.
  - External threats are outsiders or hackers including individuals, representative of foreign countries, terrorist groups, or organized crime. An outsider is an individual who does not have authorized access to an organization's computer system. Today's hackers are advanced in computer skills and have access to hacking software that provides the capability to quickly and easily identify a system's security weaknesses. Using tools available on the Internet, today's hackers are capable of running automated attack applications against thousands of computers at a time.
- To learn more about deliberate threats, the following definitions are provided for your information:
  - **Phishing:** High-tech scam that uses email or websites to deceive you into disclosing your credit card numbers, bank account information, Social Security number, passwords, or other sensitive information.
  - **Espionage:** The act of obtaining, delivering, transmitting, communication, or receiving information about the national defense with an intent, or reason to believe, that the information may be used to the injury of the United States or to the advantage of any foreign nation.
  - **Hacking:** Illegally accessing other people's computer systems for destroying, disruption, or ferrying out illegal activities on the network or computer systems.
  - **Malicious Logic:** Hardware, software, or firmware capable of performing an unauthorized function on an Information System.

- **Social Engineering:** A euphemism for non-technical or low-technology means – such as lies, impersonation, tricks, bribes, blackmail, and threats – used to attack information systems. For example, an unauthorized person who attempts to gain passwords by posing as a service technician with an urgent access problem.

## **8. User Guidance**

- The most important thing to remember is that Air Force Systems are provided for Air Force business. Unauthorized use is a violation of Air Force, Department of Defense, and government policy. Consequences for such use can be severe. There are many simple steps to protecting your system and your vital information: password discipline, backing up critical data, and securing your system when not in use.
- Here are several vital practices EVERY ONE should incorporate to their daily use of Air Force IT systems.
  - Use IT system for official AF business only--this applies to e-mail as well
    - Only use approved software
    - Don't use commercial internet service providers for official e-mail
    - Don't use commercial network for official business
  - Properly encrypt sensitive email when transmitting or storing
  - Don't share passwords
  - Don't bypass security programs to update software
    - Contact help desk for assistance
  - Back up critical files on a regular basis to minimize loss of data
  - Secure IT system when not in use
- But even with your best effort, issues still arise. The following information applies during these times:
  - Be aware of the latest efforts to attack your system.
  - Know your Unit IT system administrator.
  - Report system abnormalities
    - Slow computer performance
    - Files disappearing unexpectedly
    - Constant error messages
  - Take **Immediate Action** if you know or suspect your system has a virus
    - Contact the help desk
    - Eliminate the virus from your computer by deleting the infected file
    - Run the anti-virus protection software

## **9. Consequences of Violating System Security Measures**

- The consequences to not keeping our information safe can be devastating. At the very least, disciplinary action is one of the consequences to information assurance and information security violations. In the worst case scenario, violations lead to national security failures that put our nation and our allies at unnecessary risk. By reporting information security incidents immediately, you will help to minimize the potential damage and decrease possible risk: report incidents immediately to your Client Support Administrator (CSA) or Information Assurance Officer (IAO).

## FY2010 DoD Information Assurance Awareness Test

1. The goals of IA are to protect our information and information systems.
  - a. True
  - b. False
  
2. Environmental threats include what event:
  - a. Lightning
  - b. Fires
  - c. Floods
  - d. All of the above
  
3. What principle means that information services are accessible when they are needed?
  - a. Confidentiality
  - b. Integrity
  - c. Availability
  - d. Authentication
  - e. Non-repudiation
  
4. A hacker who attempts to gain system information from an employee by posing as a service technician or system administrator is using what type of hacking technique?
  - a. Mobile code
  - b. Social engineering
  - c. Software vulnerability
  - d. Peer-to-peer
  
5. If you discover a virus has infected your system, you should do ALL of the following except:
  - a. Contact the help desk
  - b. Email the infected file to your IAO
  - c. Eliminate the virus from your computer by deleting the infected file
  - d. Run the anti-virus scan
  
6. Which of the following is a high-tech scam that uses email or websites to deceive you into disclosing your credit card numbers, bank account information, social security number, passwords, or other sensitive information?
  - a. Phishing
  - b. Social engineering
  - c. A virus
  - d. Spyware

**"FY2010 DoD Information Assurance Awareness"  
Answer Sheet**

**Name:** \_\_\_\_\_ **Company:** \_\_\_\_\_ **Date:** \_\_\_\_\_

- 1. \_\_\_\_
- 2. \_\_\_\_
- 3. \_\_\_\_
- 4. \_\_\_\_
- 5. \_\_\_\_
- 6. \_\_\_\_



**ARNOLD ENGINEERING AND DEVELOPMENT CENTER  
INFORMATION ASSURANCE OFFICE ARNOLD AFB**

**Virus & Incident Checklist**

**VIRUS**

Contact your Information System Security Officer (ISSO) or immediate supervisor. ISSO:  
Contact NCC at 4040 Identify if the virus was downloaded from a document.

- Do NOT turn off your computer!
- Do not delete the message/file.
- Do not forward applicable email.
- Write down any errors that you observed on your system.
- Mark the computer **“DO NOT USE”**.

**INCIDENT**

If classified information is accidentally placed on your system do the Following  
**IMMEDIATELY!**

Notify, in person or via secure phone, your ISSO and the Help Desk at 4040. Follow Help Desk instructions.

- Do not delete the message/file.
- Do not forward applicable email.
- Do NOT turn off your computer!
- Mark the computer **“DO NOT USE”**.
- Have someone with the appropriate clearance physically guard the machine or secure in area cleared for same classification level.

## AEDC CUSTOMER INFORMATION ASSURANCE BRIEFING

1. Computer use at AEDC is monitored (Internet usage and sites).
2. In accordance with National Industrial Security Program Operation Manual (NISPOM) guidelines, hardware, software, and media shall be marked upon creation with the classification level clearly indicated. Also, all data with military application requires distribution statements, export control warning notices, and destruction notices, as directed by the appropriate DoD User Agency.
3. Software, media, equipment, or other materials shall not be removed from AEDC without proper authorization and instruction.
4. Passwords for computers that connect to any AEDC resource must consist of fifteen (15) characters (2 upper case, 2 lower case, 2 numbers and 2 special characters (@&+! etc). **Do not write passwords down.**
5. Passwords for computers that connect to any AEDC resource must be changed every sixty- (60) days.
6. **Use password-protected** screen savers and ***immediately*** activate whenever computers are left unattended.

**NOTE: WHEN THIS PAGE IS COMPLETED, IT CONTAINS PRIVACY ACT INFORMATION**

Complete this page and Fax to (931)-454-3581, ATTN: Barbara Casey, if you have any questions, please call (931)-454-3941. This is being faxed to a NISPOM-approved **Closed** area.

**Customer Information and Compliance Signature**

Citizenship: \_\_\_\_\_

AEDC POC/Sponsor: \_\_\_\_\_

Print Last Name: \_\_\_\_\_

Print First Name: \_\_\_\_\_

Middle Initial (if any): \_\_\_\_\_

Company Name: \_\_\_\_\_

Company Address: \_\_\_\_\_

Company City, State: \_\_\_\_\_

Business Telephone Number: ( \_\_\_\_\_ ) - \_\_\_\_\_

Job Title: \_\_\_\_\_

E-Mail Address: \_\_\_\_\_

**By signing below, I have read, understand, and agree to comply with the AEDC Information Assurance briefing as stipulated herein, and as addressed in the DoD Information Assurance training, which I have completed, to include the examination.**

Signature \_\_\_\_\_ Date \_\_\_\_\_

**Notice: This page contains Privacy Act Information of 1974.**

**U. S. Visitor/Customer Request to Connect *Company-Owned* Portable Electronic Device (PED) to AEDC Computer Systems/Networks or Internet**  
 (This page is not required if you are **not** connecting to AEDC Computer/Network Resources or the Internet).

PEDs include company-owned laptop computers, handheld computers, personal digital assistants (PDAs), bar code readers, and cellular telephones, etc.

To avoid delays at Pass & Registration, this page must be completed and faxed (931)-454-3581 to the ATA/IA Office, ATTN: Barbara Casey, prior to your visit.

<b>Name of PED User:</b>	
<b>Type of PED:</b>	
<b>PED Manufacturer &amp; Model Number:</b>	
<b>PED Serial Number:</b>	
<b>Does your laptop have wireless capability (Bluetooth, WiFi, IR)?</b> <small>PCs/laptops with wireless technology installed will have that capability disabled and IR ports will be covered with metallic tape prior to being used at AEDC</small>	<b>Underline:      YES      NO</b>
<b>MAC addresses of Hard-Wired and Wireless Adaptor (Bluetooth, WiFi)</b> <small>See instructions on next page for determining MAC addresses and fax results with this page.</small>	<b>Hard-Wired:</b>
	<b>Wireless:</b>
<b>Is the PED company/government owned?</b> (Personally owned PEDs are <b>not</b> authorized for use at AEDC)	
<b>Name of company/organization which owns the PED:</b>	
<b>Location where the PED computer will be used at AEDC:</b>	
<b>Length of time authorization is required</b>  <div style="text-align: right;"> <b>Start Date:</b>  <b>End Date:</b> </div>	
<b>PED connectivity to any AEDC computer system or network is <b>authorized only with additional AF approval.</b></b>	
<b>Purpose for which PED will be used?</b>	
<b>Is Internet access required?</b>	<b>Underline:      YES      NO</b>
<b>Is a Virtual Private Network (VPN) Required?</b>	<b>Underline:      YES      NO</b>
<b>USAF/Aerospace Testing Alliance (ATA) Point of Contact</b>	

# General Information about Connectivity at AEDC and Basic Steps for Finding and Documenting Wired and Wireless MAC Addresses

## Network

Internet connectivity:

- Active 10/100 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 to use Transport Control Protocol (TCP) and/or User Datagram Protocol (UDP)/Internet Protocol version 4(IPv4).
- Configured for Dynamic Host Configuration Protocol (DHCP) for both IP addressing and Domain Name Service (DNS).

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

The AEDC IA section will need your Media Access Control (MAC) address for your device(s) Ethernet port(s) when you make initial application for equipment approval and connection.

### **Wired LAN Procedure: Make sure your wired LAN interface is enabled**

- 1) Open a command window:  
-> START -> Run -> Type "CMD" and press Enter
- 2) At the command prompt in command window, type **ipconfig /all >> laninfo.txt** and press "Enter"
- 3) Text file will be generated to area where indicated by C: prompt in command screen (i.e., C:\Documents and Setting\YOUR-NAME)

Additionally, please have your AEDC POC check with the AEDC Network Infrastructure Engineering section so that network connectivity can be confirmed or installed in your AEDC work area prior to your arrival. Generally 30 days lead time is sufficient to make allowance for this inquiry.

## Wireless

- Operation of any sort of wireless communication technology associated with customer owned computing equipment is strictly prohibited in all AEDC test areas. Test customers are required to disable all such wireless interfaces and insure they remain disabled while on base.

The AEDC IA section will need your Media Access Control (MAC) address for your device(s) wireless interfaces when you make initial application for equipment approval and connection.

### **Wireless LAN Procedure: Make sure your wireless LAN interface is enabled**

- 1) Open a command window:  
-> START -> Run -> Type "CMD" and press Enter
- 2) At the command prompt in command window, type **ipconfig /all >> wlaninfo.txt** and press "Enter"
- 3) Text file will be generated to area where indicated by C: prompt in command screen (i.e., C:\Documents and Setting\YOUR-NAME)

Please inform your IT department of these requirements so they can configure your device appropriately such that all wireless interfaces are removed or disabled or that you have access permissions to disable the interfaces while on base.

**Fax both text files with PED pass request on previous page.**

## Identifying Wireless Capabilities

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



- ❑ 2. A wireless network connection icon, like that shown on the left side of the system tray below, indicates that the laptop does support wireless networking.



- ❑ 3. A logo sticker on the laptop like those below indicates it **may** support wireless networking.



- ❑ 4. 802.11 can either be mini-PCIs located beneath a removable panel on the laptop's underside, as shown in the figure below, or external cards that plug into PCMCIA, Compact Flash, Secure Digital, Ethernet, or USB interfaces. **These external cards must be physically removed while in NSA spaces.**



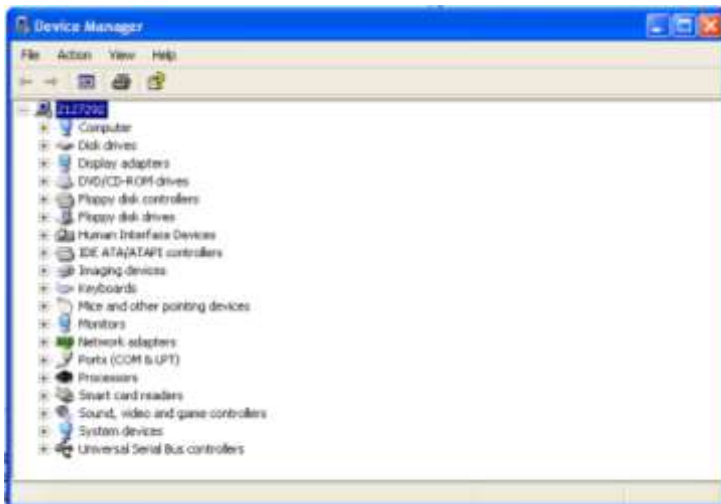
- ❑ 5. Small dark red plastic windows on the laptop indicated infrared capabilities. These windows **must** be completely covered with metallic tape.
- ❑ 6. Although not a wireless issue, laptops have internal microphones that **must** be disabled using a 3.5-mm erasing plug inserted into the external microphone jack.

## Disabling Wireless in Windows

- 1. Log on as an administrator.\*
- 2. Open the **Start Menu**.
- 4. If not using XP, open **Setting**. If using XP, skip to step 4.
- 4. Open the **Control Panel**.
- 5. If using XP in the Category view, click **Performance and Maintenance**, otherwise skip to Step 6.



- 6. Double-click on the **System** icon
- 7. Select the **Hardware** tab
- 8. Click the **Device Manager** button.



- 9. Click the + sign to the left of the Bluetooth device, right click on the Bluetooth adapter, and select **Disable**.
- 10. Click the + sign to the left of the **Network adapters**, right click on the **wireless adapter**, and select **Disable**.
- 11. For Windows XP:
  - a. Open the **Start Menu**.
  - b. Open the **Administrative Tools**.
  - c. Open **Services**.
  - d. In the right pane, double-click the **Wireless Zero Configuration** service.
  - e. Under **Startup type**, select **Disabled** from the pull down menu.
  - f. Under **Service Status**, click the **Stop** button.
  - g. Once the service has stopped, click OK to finish.

## ***Disabling Wireless in Linux***

(Applies only to Fedora Core 3)

- ❑ 1. Log on as *root* user (only root has the permissions to run the following commands).\*
- ❑ 2. Open a command prompt (xterm, shell tool, cmd tool, etc.)
- ❑ 3. Issue the command **ifconfig -a** to get a listing of available network interfaces.
- ❑ 4. Decide which interface(s) to disable. Anything with **wlan** or **wifi** in the interface name is most likely wireless, but sometimes interfaces such as **eth1** are as well.
- ❑ 5. Run the command

**ifconfig [interface] down**

To disable an interface, run this command for all interfaces that need to be disabled using Step 3.

Example: `ifconfig wlan() down`

When the computer is returned to an area approved for wireless networks issue the following command to enable the wireless adapter:

**ifconfig [interface] up**

## Test Customers Requesting VPN Access at AEDC

To have adequate time to process the change request for our firewalls specified by our Configuration Management process to provide access to test customers requesting VPN access while at AEDC, the following information is required at least two weeks before access is needed. For any assistance with this page only, please contact Adam Prince (931-454-4979/DSN 340-4979) or Mary Knight (931-454-6845/DSN 340-6845).

### Test Customer VPN Request (fill out shaded entries only)

<b>Company</b>	
<b>Date of Request</b>	
<b>ATA or Government Sponsor</b>	
<b>ATA or Government Organization</b>	
<b>Date Required</b>	
<b>Duration</b>	
<b>Test or Support Purpose</b>	
<b>Mission Impact</b> (Define in detail, the specific impact if customer access to the VPN device from AEDC networks cannot be granted.)	
<b>Customer Name</b>	
<b>Customer Email</b>	
<b>MAC Address</b> (This is the <b>physical</b> identification of the network card of your device; NOT wireless addresses. Should look something like: 00-0E-F4-S3-R0-EE)	
<b>Approving Organization</b>	
<b>ATA or Govt Sponsor's Approval</b>	
<b>Final Approver</b>	
<b>Approval Date</b>	
<b>Approval Type</b>	<Interim or Final>
<b>Admin/Date added to FW</b>	

### VPN Requirements

Internet Protocol Address (An IP address is the 4 Octet unique address associated with the VPN endpoint device where you are connecting; i.e., 111.111.111.111 would be associated with Customer.VPN.Company.com.)	Port/Protocol Service (This is the transmission mechanism for connecting to the endpoint site. Common ports are 443, 4500, 500, etc.)	Crossed Boundaries	PPS Color

**“FY 2010 DoD Information Assurance Awareness”**

**Answers**

1. a
2. d
3. c
4. b
5. b
6. a