

25U COURSE REQUIREMENTS

-
- DOD CYBER AWARENESS CHALLENGE TRAINING
MODULE
 - INFORMATION ASSURANCE FUNDAMENTALS
FORMALLY KNOWN AS THE IASO
 - SIGNED AUP

[-https://ia.signal.army.mil/DoDIAA/](https://ia.signal.army.mil/DoDIAA/)

Login to take the DOD Cyber Awareness Challenge Training

https://ia.signal.army.mil/DoDIAA/ Information Assurance Trai... x

File Edit View Favorites Tools Help

HOME LOGIN COURSES MTT LOCATIONS RESOURCES CONTACT

INFORMATION ASSURANCE TRAINING CENTER
US ARMY SIGNAL CENTER FORT GORDON, GA

DoD Cyber Awareness Challenge Training

Objectives: The objectives of this training are listed as follows.

- Affect physical security of computer hardware and software.
- Limit access to computer equipment to authorized users only.
- Prevent computer fraud, waste and abuse.
- Implement effective contingency planning.
- Report security problems to the chain of command.
- Protect computer files from infection by malicious logic.

Note:

- To meet Army requirements, all personnel must complete the training and score 70% or greater on the Cyber Awareness Challenge test.
- One certificate will be generated upon successful completion of the training and test. This certificate will have the SIT Director's signature preprinted on it.
 - This training meets the requirement until version 2 is implemented for FY14.

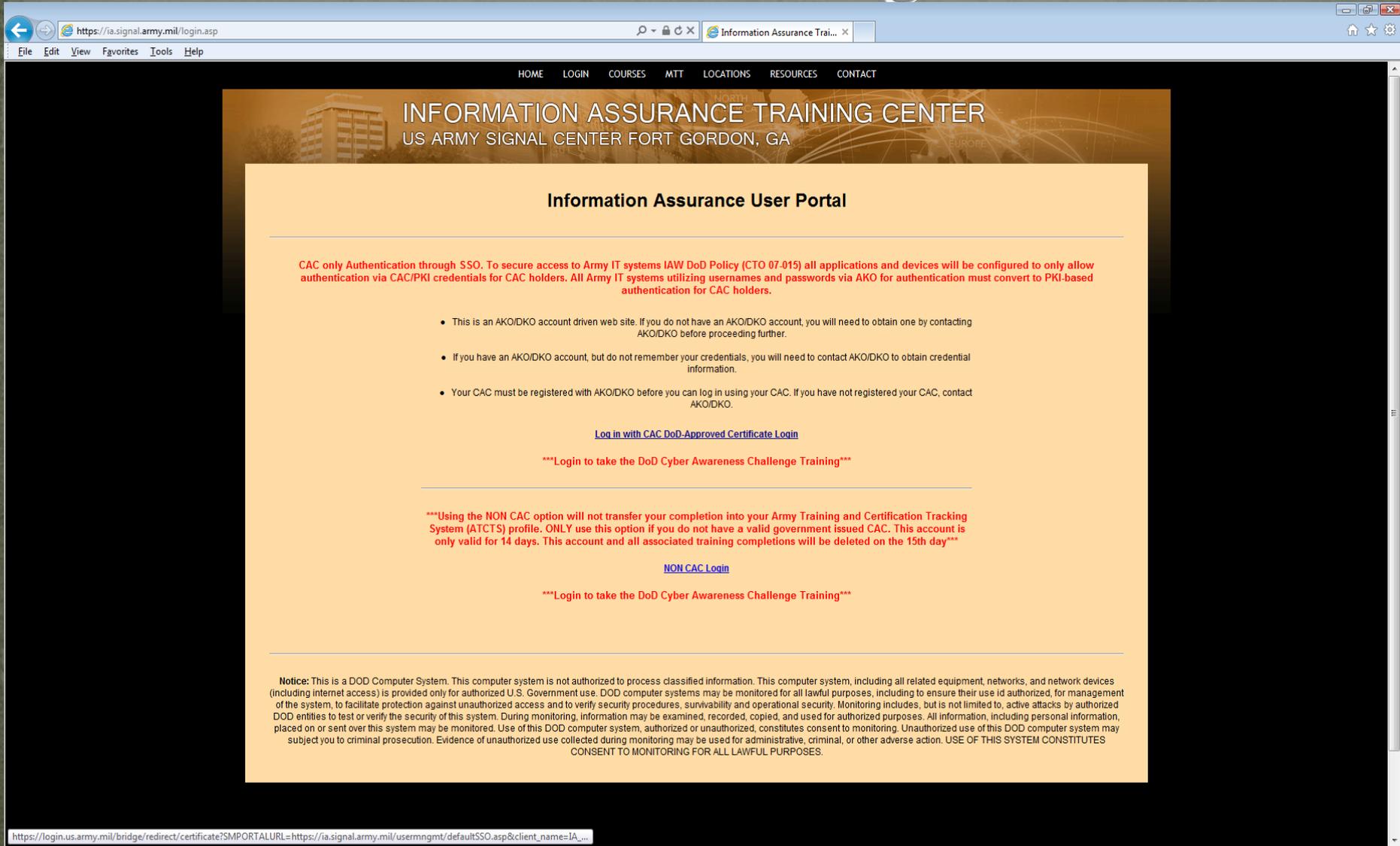
All personnel must successfully complete the training and the end of course test to receive full credit :

Login to take the DoD Cyber Awareness Challenge Training

Army is moving to one certificate

Personnel = Anyone accessing an Army network.

Login with CAC DoD-Approved Certificate Login



The screenshot shows a web browser window with the URL <https://ia.signal.army.mil/login.asp>. The page title is "Information Assurance Training Center". The navigation menu includes: HOME, LOGIN, COURSES, MTT, LOCATIONS, RESOURCES, CONTACT.

INFORMATION ASSURANCE TRAINING CENTER

US ARMY SIGNAL CENTER FORT GORDON, GA

Information Assurance User Portal

CAC only Authentication through SSO. To secure access to Army IT systems IAW DoD Policy (CTO 07-015) all applications and devices will be configured to only allow authentication via CAC/PKI credentials for CAC holders. All Army IT systems utilizing usernames and passwords via AKO for authentication must convert to PKI-based authentication for CAC holders.

- This is an AKO/DKO account driven web site. If you do not have an AKO/DKO account, you will need to obtain one by contacting AKO/DKO before proceeding further.
- If you have an AKO/DKO account, but do not remember your credentials, you will need to contact AKO/DKO to obtain credential information.
- Your CAC must be registered with AKO/DKO before you can log in using your CAC. If you have not registered your CAC, contact AKO/DKO.

[Log in with CAC DoD-Approved Certificate Login](#)

*****Login to take the DoD Cyber Awareness Challenge Training*****

*****Using the NON CAC option will not transfer your completion into your Army Training and Certification Tracking System (ATCTS) profile. ONLY use this option if you do not have a valid government issued CAC. This account is only valid for 14 days. This account and all associated training completions will be deleted on the 15th day*****

[NON CAC Login](#)

*****Login to take the DoD Cyber Awareness Challenge Training*****

Notice: This is a DOD Computer System. This computer system is not authorized to process classified information. This computer system, including all related equipment, networks, and network devices (including internet access) is provided only for authorized U.S. Government use. DOD computer systems may be monitored for all lawful purposes, including to ensure their use is authorized, for management of the system, to facilitate protection against unauthorized access and to verify security procedures, survivability and operational security. Monitoring includes, but is not limited to, active attacks by authorized DOD entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied, and used for authorized purposes. All information, including personal information, placed on or sent over this system may be monitored. Use of this DOD computer system, authorized or unauthorized, constitutes consent to monitoring. Unauthorized use of this DOD computer system may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal, or other adverse action. USE OF THIS SYSTEM CONSTITUTES CONSENT TO MONITORING FOR ALL LAWFUL PURPOSES.

https://login.us.army.mil/bridge/redirect/certificate?SMPORTALURL=https://ia.signal.army.mil/usermgmt/defaultSSO.asp&client_name=IA_...

Put in the correct information for your Branch, Type, and MACOM

Information Assurance User Portal

Welcome Jared Phares

You have successfully logged in.

To continue, you must update your record. Please complete the following form so that your record can be updated. All fields are MANDATORY.

Select a Branch:

Select a Type:

Select a MACOM:

Click [Here](#) to log out.

Notice: This is a DOD Computer System. This computer system is not authorized to process classified information. This computer system, including all related equipment, networks, and network devices (including internet access) is provided only for authorized U.S. Government use. DOD computer systems may be monitored for all lawful purposes, including to ensure their use is authorized, for management of the system, to facilitate protection against unauthorized access and to verify security procedures, survivability and operational security. Monitoring includes, but is not limited to, active attacks by authorized DOD entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied, and used for authorized purposes. All information, including personal information, placed on or sent over this system may be monitored. Use of this DOD computer system, authorized or unauthorized, constitutes consent to monitoring. Unauthorized use of this DOD computer system may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal, or other adverse action. USE OF THIS SYSTEM CONSTITUTES CONSENT TO MONITORING FOR ALL LAWFUL PURPOSES.

Click on take exam

Information Assurance User Portal

Welcome Jared Phares

Thank you for updating your account.

To take the training for DoD Information Assurance Awareness or Information Assurance Fundamentals exams, click on the Courses menu link above.

[DOD Cyber Awareness Challenge](#)

[Take an exam](#)

[View Scores and Print Certificates](#)

[View and Sign AUP](#)

[Fort Gordon Data at Rest validation](#)

Click [Here](#) to log out.

Notice: This is a DOD Computer System. This computer system is not authorized to process classified information. This computer system, including all related equipment, networks, and network devices (including internet access) is provided only for authorized U.S. Government use. DOD computer systems may be monitored for all lawful purposes, including to ensure their use is authorized, for management of the system, to facilitate protection against unauthorized access and to verify security procedures, survivability and operational security. Monitoring includes, but is not limited to, active attacks by authorized DOD entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied, and used for authorized purposes. All information, including personal information, placed on or sent over this system may be monitored. Use of this DOD computer system, authorized or unauthorized, constitutes consent to monitoring. Unauthorized use of this DOD computer system may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal, or other adverse action. USE OF THIS SYSTEM CONSTITUTES CONSENT TO MONITORING FOR ALL LAWFUL PURPOSES.

Take DOD Cyber Awareness Challenge training Module and Information Assurance Fundamentals Formally known as the IASO

The screenshot shows a web browser window with the URL <https://ia.signal.army.mil/usermgmt/examPage1.SSO.asp>. The browser's address bar also displays "Information Assurance Trai...". The browser's menu bar includes "File", "Edit", "View", "Favorites", "Tools", and "Help". The website's navigation menu includes "HOME", "LOGIN", "COURSES", "MTT", "LOCATIONS", "RESOURCES", and "CONTACT".

Information Assurance User Portal

Test Selection

To take one of the training exams, click go! to proceed.

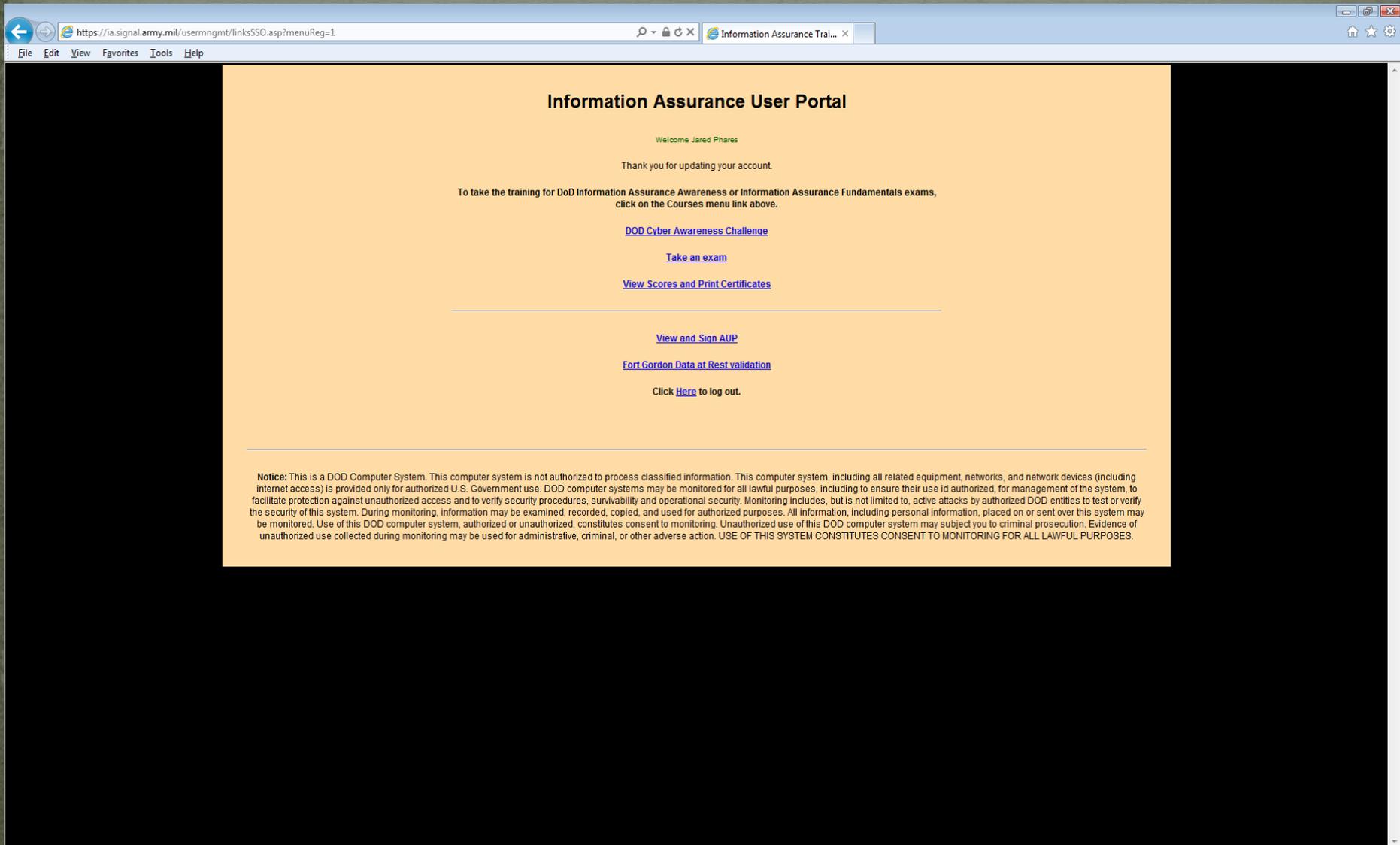
Exam Name
DOD Cyber Awareness Challenge Training Module Go!
Information Assurance Fundamentals Formally known as the (IASO) go!
Phishing Training go!

[Go Back To User Menu](#)

Click [Here](#) to log out.

Note: The Annual Cyber Awareness challenge exam is only accessible at the end of the training module. If you score less than 70% on the exam you will have to complete the training prior to retesting.

After completion of the exams view scores and print certificates for each exam and present to your unit and the 25U instructors



The screenshot shows a web browser window with the address bar displaying <https://ia.signal.army.mil/usermgmt/linksSSO.asp?menuReg=1>. The browser title is "Information Assurance Trai...". The page content is as follows:

Information Assurance User Portal

Welcome Jared Phares

Thank you for updating your account.

To take the training for DoD Information Assurance Awareness or Information Assurance Fundamentals exams, click on the Courses menu link above.

[DOD Cyber Awareness Challenge](#)

[Take an exam](#)

[View Scores and Print Certificates](#)

[View and Sign AUP](#)

[Fort Gordon Data at Rest validation](#)

Click [Here](#) to log out.

Notice: This is a DOD Computer System. This computer system is not authorized to process classified information. This computer system, including all related equipment, networks, and network devices (including internet access) is provided only for authorized U.S. Government use. DOD computer systems may be monitored for all lawful purposes, including to ensure their use is authorized, for management of the system, to facilitate protection against unauthorized access and to verify security procedures, survivability and operational security. Monitoring includes, but is not limited to, active attacks by authorized DOD entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied, and used for authorized purposes. All information, including personal information, placed on or sent over this system may be monitored. Use of this DOD computer system, authorized or unauthorized, constitutes consent to monitoring. Unauthorized use of this DOD computer system may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal, or other adverse action. USE OF THIS SYSTEM CONSTITUTES CONSENT TO MONITORING FOR ALL LAWFUL PURPOSES.

The view exams and Print screen looks like this once completed with certain training

The screenshot shows a web browser window with the URL <https://ia.signal.army.mil/usermgmt/examScoresCertsSSO.asp>. The page title is "Information Assurance User Portal". Below the title, there is a sub-header "Scores and Certificates" and a message: "To print your certificate, click the View Certificate link".

The main content is divided into three sections:

- Signed AUP**: A table with one row showing "AUP" and "Signed Date: 8/24/2013 12:29:58 PM", with a "View AUP" link.
- Certificates for Online Training**: A message "ONLY successfully completed exam information will be displayed below. Exams with scores below 70 will not appear." followed by a table of exam results.
- Certificates for In-Class Training**: A table with one row showing "Functional Network+ 005 -13" and "5/13/2013 - 5/17/2013", with a "View Certificate" link.

At the bottom, there are links for "Go Back To User Menu" and "Click [Here](#) to log out."

Module Tested	Date Taken	Final Score	Certificate
Phishing Training	8/5/2011 7:07:46 PM	70	View Certificate
OPSEC and Safe Social Networking	8/5/2011 7:10:14 PM	90	View Certificate
IAF (Mgt Level 1)	6/19/2013 2:20:00 PM	80	View Certificate
Annual DoD Cyber Awareness Challenge Exam	10/24/2013 10:20:47 AM	90	View Certificate

Class Taken	Class Dates	Certificate
Functional Network+ 005 -13	5/13/2013 - 5/17/2013	View Certificate

Go to View and Sign AUP

Information Assurance User Portal

Welcome Jared Phares

Thank you for updating your account.

To take the training for DoD Information Assurance Awareness or Information Assurance Fundamentals exams, click on the Courses menu link above.

[DOD Cyber Awareness Challenge](#)

[Take an exam](#)

[View Scores and Print Certificates](#)

[View and Sign AUP](#)

[Fort Gordon Data at Rest validation](#)

Click [Here](#) to log out.

Notice: This is a DOD Computer System. This computer system is not authorized to process classified information. This computer system, including all related equipment, networks, and network devices (including internet access) is provided only for authorized U.S. Government use. DOD computer systems may be monitored for all lawful purposes, including to ensure their use is authorized, for management of the system, to facilitate protection against unauthorized access and to verify security procedures, survivability and operational security. Monitoring includes, but is not limited to, active attacks by authorized DOD entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied, and used for authorized purposes. All information, including personal information, placed on or sent over this system may be monitored. Use of this DOD computer system, authorized or unauthorized, constitutes consent to monitoring. Unauthorized use of this DOD computer system may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal, or other adverse action. USE OF THIS SYSTEM CONSTITUTES CONSENT TO MONITORING FOR ALL LAWFUL PURPOSES.

Click on digitally sign

https://ia.signal.army.mil/usermgmt/ssotest/aupsig.asp

File Edit View Favorites Tools Help

f. I will not attempt to access or process data exceeding the authorized IS classification level.

g. I will not alter, change, configure, or use operating systems or programs, except as specifically authorized.

h. I will not introduce executable code (such as, but not limited to, .exe, .com, .vbs, or .bat files) without authorization, nor will I write malicious code.

L. I will safeguard and mark with the appropriate classification level all information created, copied, stored, or disseminated from the IS and will not disseminate it to anyone without a specific need to know.

j. I will not utilize Army- or DoD-provided ISs for commercial financial gain or illegal activities.

k. Maintenance will be performed by the System Administrator (SA) only.

l. I will use screen locks and log off the workstation when departing the area.

m. I will immediately report any suspicious output, files, shortcuts, or system problems to the Organizations System Administrator and/or Information Assurance Support Officer and cease all activities on the system.

n. I will address any questions regarding policy, responsibilities, and duties to the organizations System Administrator and/or Information Assurance Support Officer.

o. I understand that each IS is the property of the Army and is provided to me for official and authorized uses. I further understand that each IS is subject to monitoring for security purposes and to ensure that use is authorized. I understand that I do not have a recognized expectation of privacy in official data on the IS and may have only a limited expectation of privacy in personal data on the IS. I realize that I should not store data on the IS that I do not want others to see.

p. I understand that monitoring of Classified Network and Unclassified Network will be conducted for various purposes and information captured during monitoring may be used for administrative or disciplinary actions or for criminal prosecution. I understand that the following activities define unacceptable uses of an Army IS:

- to show what is not acceptable use
- to show what is acceptable during duty/non-duty hours
- to show what is deemed proprietary or not releasable (key word or data identification)
- to show what is deemed unethical (e.g., spam, profanity, sexual content, gaming)
- to show unauthorized sites (e.g., pornography, streaming video, E-Bay)
- to show unauthorized services (e.g., peer-to-peer, distributed computing)
- to define proper email use and restrictions (e.g., mass mailing, hoaxes, auto forwarding)
- to explain expected results of policy violations (1 st, 2 nd, 3rd, etc)

(Note: Activity in any criteria can lead to criminal offenses.)

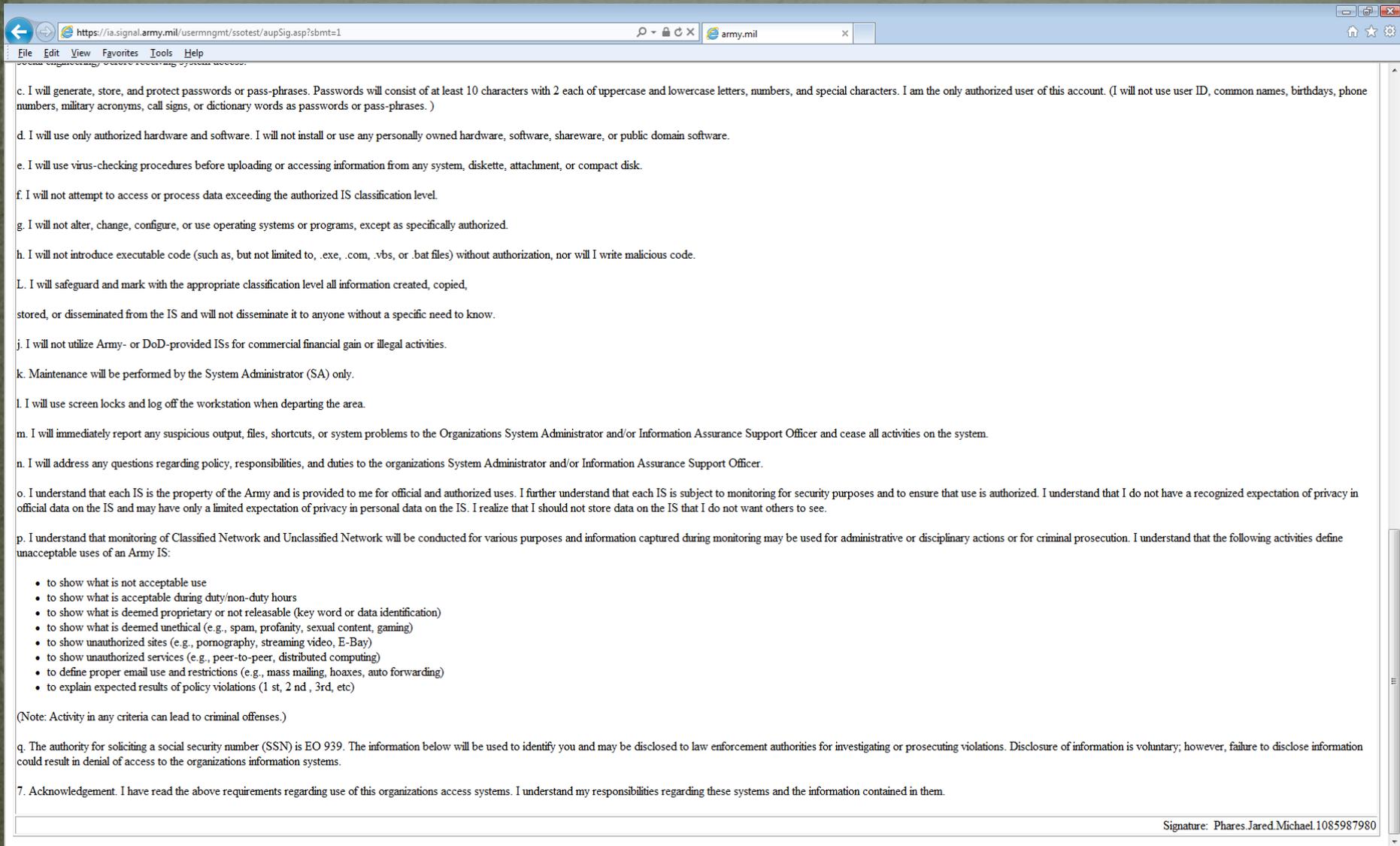
q. The authority for soliciting a social security number (SSN) is EO 939. The information below will be used to identify you and may be disclosed to law enforcement authorities for investigating or prosecuting violations. Disclosure of information is voluntary; however, failure to disclose information could result in denial of access to the organizations information systems.

7. Acknowledgement. I have read the above requirements regarding use of this organizations access systems. I understand my responsibilities regarding these systems and the information contained in them.

[Acronyms](#)

Click to digitally sign

Once digitally signed it will look like picture below and print present copy to your unit and to your 25U instructor



The image shows a screenshot of a web browser window. The address bar displays the URL: <https://ia.signal.army.mil/usermgmt/ssotest/aupSig.asp?sbmt=1>. The browser window contains a list of system usage requirements, numbered c through 7. The requirements cover password policies, hardware and software usage, virus checking, data access, system modifications, code execution, information safeguarding, commercial use, maintenance, screen locks, reporting, policy questions, monitoring, and social security number solicitation. A signature is visible at the bottom right of the page.

c. I will generate, store, and protect passwords or pass-phrases. Passwords will consist of at least 10 characters with 2 each of uppercase and lowercase letters, numbers, and special characters. I am the only authorized user of this account. (I will not use user ID, common names, birthdays, phone numbers, military acronyms, call signs, or dictionary words as passwords or pass-phrases.)

d. I will use only authorized hardware and software. I will not install or use any personally owned hardware, software, shareware, or public domain software.

e. I will use virus-checking procedures before uploading or accessing information from any system, diskette, attachment, or compact disk.

f. I will not attempt to access or process data exceeding the authorized IS classification level.

g. I will not alter, change, configure, or use operating systems or programs, except as specifically authorized.

h. I will not introduce executable code (such as, but not limited to, .exe, .com, .vbs, or .bat files) without authorization, nor will I write malicious code.

L. I will safeguard and mark with the appropriate classification level all information created, copied, stored, or disseminated from the IS and will not disseminate it to anyone without a specific need to know.

j. I will not utilize Army- or DoD-provided ISs for commercial financial gain or illegal activities.

k. Maintenance will be performed by the System Administrator (SA) only.

l. I will use screen locks and log off the workstation when departing the area.

m. I will immediately report any suspicious output, files, shortcuts, or system problems to the Organizations System Administrator and/or Information Assurance Support Officer and cease all activities on the system.

n. I will address any questions regarding policy, responsibilities, and duties to the organizations System Administrator and/or Information Assurance Support Officer.

o. I understand that each IS is the property of the Army and is provided to me for official and authorized uses. I further understand that each IS is subject to monitoring for security purposes and to ensure that use is authorized. I understand that I do not have a recognized expectation of privacy in official data on the IS and may have only a limited expectation of privacy in personal data on the IS. I realize that I should not store data on the IS that I do not want others to see.

p. I understand that monitoring of Classified Network and Unclassified Network will be conducted for various purposes and information captured during monitoring may be used for administrative or disciplinary actions or for criminal prosecution. I understand that the following activities define unacceptable uses of an Army IS:

- to show what is not acceptable use
- to show what is acceptable during duty/non-duty hours
- to show what is deemed proprietary or not releasable (key word or data identification)
- to show what is deemed unethical (e.g., spam, profanity, sexual content, gaming)
- to show unauthorized sites (e.g., pornography, streaming video, E-Bay)
- to show unauthorized services (e.g., peer-to-peer, distributed computing)
- to define proper email use and restrictions (e.g., mass mailing, hoaxes, auto forwarding)
- to explain expected results of policy violations (1 st, 2 nd, 3rd, etc)

(Note: Activity in any criteria can lead to criminal offenses.)

q. The authority for soliciting a social security number (SSN) is EO 939. The information below will be used to identify you and may be disclosed to law enforcement authorities for investigating or prosecuting violations. Disclosure of information is voluntary; however, failure to disclose information could result in denial of access to the organizations information systems.

7. Acknowledgement. I have read the above requirements regarding use of this organizations access systems. I understand my responsibilities regarding these systems and the information contained in them.

Signature: Phares.Jared.Michael.1085987980

**ALL CERTIFICATES AND SIGNED
AUP MUST BE COMPLETED WITHIN
THE CURRENT YEAR TO BE
ACCEPTED!!!!!!!**