HQ, USAES In-Processing Checklist

Rank/ Grade Full Name:
Date In-Processed:

Links:

- ☐ Information Awareness Training Certificate- https://ia.signal.army.mil/login.asp
- ☐ Acceptable Use Policy- https://ia.signal.army.mil/login.asp
- ☐ Classified Information Non-Disclosure Agreement
- ☐ E-qip Investigation Request – https://nbib.opm.gov/e-qip-background-investigations/
- ☐
- ☐ Antiterrorism Training (AT Level 1)- https://jkodirect.jten.mil
- ☐ Annual Security Refresher Training –https://www.lms.army.mil
- ☐ TRADOC NATO Briefing Acknowledgement (Digital)

Optional:

- ☐ Blackberry Device Training – http://iatraining.disa.mil/eta/smartphone_tablet_v2/launchpage.htm
- ☐ SERE Training (OCONUS Travel)- https://jkodirect.jten.mil
- ☐ OER/NCOER
- ☐ ORB/ERB
- ☐ APFT
- ☐ ORDERS
- ☐ Cup and Flower Fund _POC: OPS

SIPRNet

- ☐ SIPR Request (DD Form 2875, DD Form 2842, and SIPR Memo enclosed)
- ☐ NATO SIPR Brief
- ☐ Derivative Classification Training – http://cdsetrain.dtic.mil/derivative/index.htm

In-Processing:

- ☐ ATCTS – Date:
- ☐ DTS – Date:
- ☐ JPAS – Date:
- ☐ Mail Lists – Date:
- ☐ UMS – Date:
- ☐ IA Training-Date:
- ☐ AUP – Date:
- ☐

Security Clearance:

- ☐ Investigation Type:_____ Date:_____
- ☐ Clearance Type:_____Date:_____

If you have any questions, please contact:

Sherri L. Wallace
Administrative Support Assistant
1(573) 563-8080

PERSONNEL TO BE HAILED	
RANK & NAME	
DUTY POSITION	
UNIT	
NAME OF SPOUSE	
NAME AND AGE OF CHILDREN	
PREVIOUS ASSIGNMENTS (last three)	
HOBBIES	

PERSONNEL TO BE FAREWELLED	
RANK & NAME	
PRESENT POSITION	
UNIT	
NAME OF SPOUSE	
NAME AND AGE OF CHILDREN	
DEPARTURE DATE	
NEXT ASSIGNMENT & LOCATION	
HOBBIES	

YOUR ORG In Processing

Name: _____

Grade: _____

SSN: _____

DOB: _____

Section Assigned: _____

Work Phone: _____

Mailing Address: _____

_____

Home / Cell Phone: _____

Emergency Contact Name: _____

Emergency Contact Phone: _____

PER AR 380-53 AND TASKING IN517481

ATTENTION!
DO NOT PROCESS, STORE, OR TRANSMIT CLASSIFIED INFORMATION ON NONSECURE TELECOMMUNI-CATIONS SYSTEMS. OFFICIAL DOD TELECOMMUNI-CATIONS SYSTEMS - INCLUDING TELEPHONES, FACSIMILE MACHINES, COMPUTER NETWORKS, AND MODEMS - ARE SUBJECT TO MONITORING FOR TELECOMMUNICATIONS SECURITY PURPOSES AT ALL TIMES. USE OF OFFICIAL DOD TELECOMMUNICA-TIONS SYSTEMS CONSTITUTES CONSENT TO INFORMATION SYSTEMS SECURITY MONITORING.

FOR INTERNAL USE ONLY	
In process date:	
Personnel Roster	
Work Phone Roster	
Add DOB to Calendar	
Add/Change Form 2875 for ATAAPS Access	
Initial OPSEC Brief/30 Days	

I acknowledge the above statement: _____Initials _____Date

ADDITIONAL INFORMATION FOR USAES SOCIAL ROSTER

SPOUSE NAME/NICKNAME _____

SPOUSE EMAIL _____

SPOUSE BIRTHDATE _____

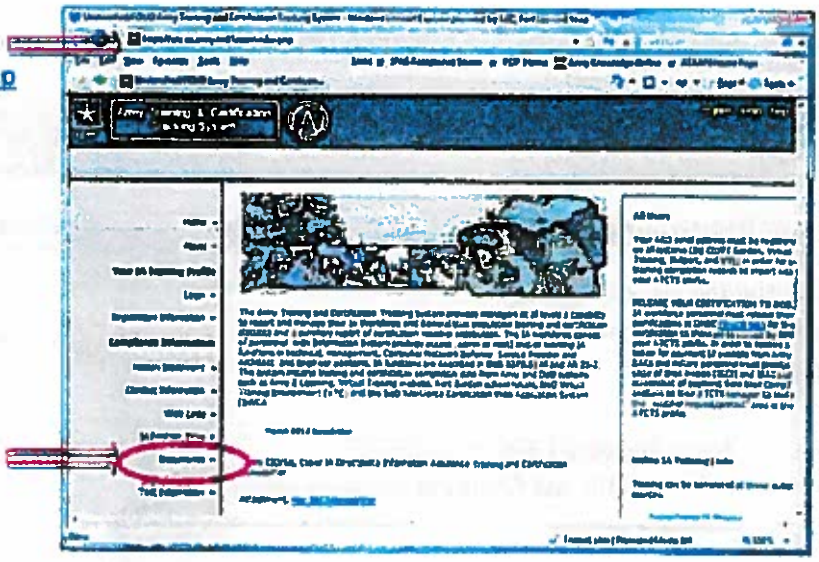
ANNIVERSARY DATE _____

Follow these steps to complete your user agreement. After signing and uploading to ATCTS, print a hard copy and turn in to Ms. Booth.

Army Training & Certification Tracking System (ATCTS)

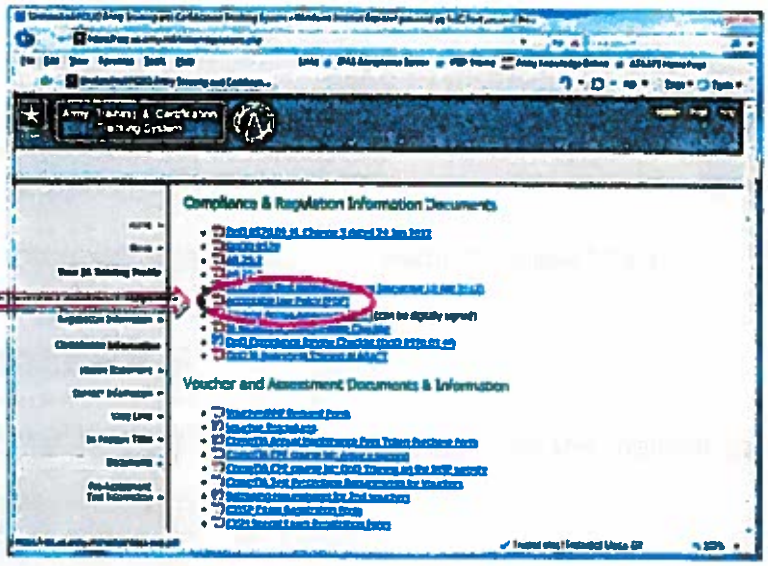
Date Completed: _____

1 Go to: https://atc.us.army.mil/iastar/index.php



2 Select "Documents"

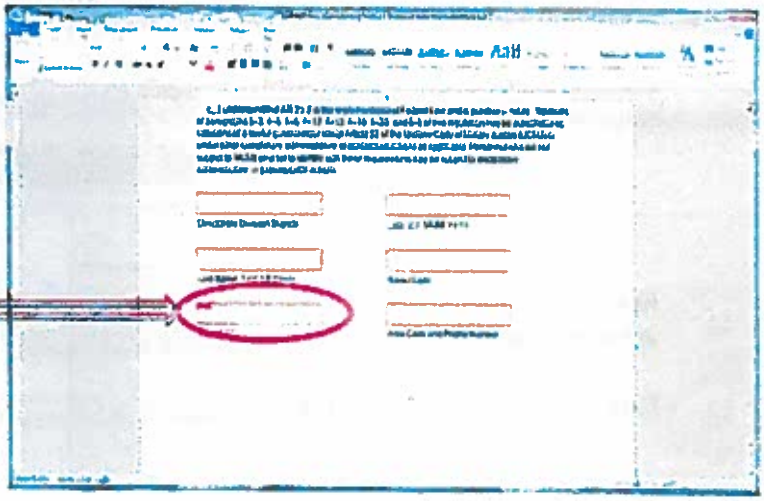
3 Select "Acceptable Use Policy"



ACCEPTABLE USE POLICY (AUP) opens in PDF.

4 Enter requested data on page 8.

5 Apply e-Signature.



6 Save the AUP as a PDF to the desktop.

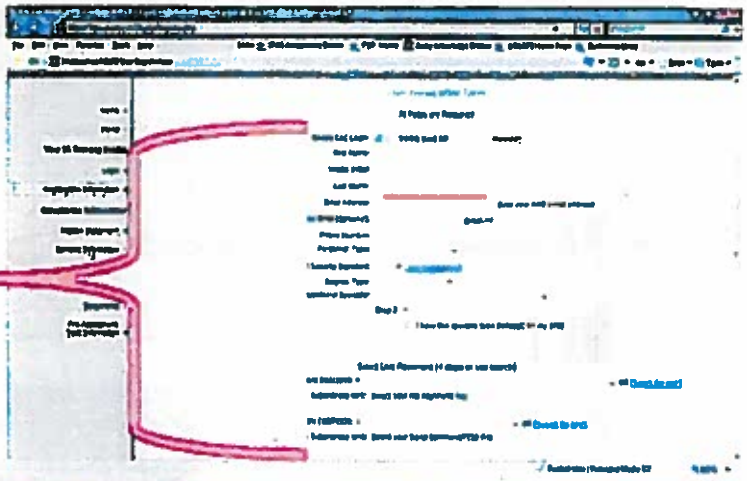
Close out  **of the ACCEPTABLE USE POLICY (AUP) PDF and return to the ATCTS web page.**

7 Click on " register " button.

User Registration Form page opens.

(Consult the Security Manager / IAO if needed for assistance in providing the correct data requested.)

8 Apply requested data in appropriate fields. NOTE: ALL Fields are required.



Scroll down to bottom of page

9 Click " Register " button.

Registration Sent page opens.

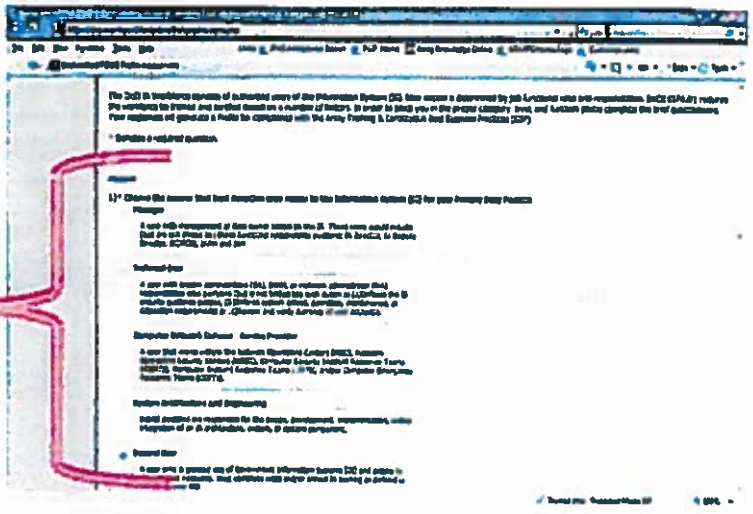
10 Click on "**click here** " link.

Acknowledgement page opens.

11 Read and check acknowledgement.

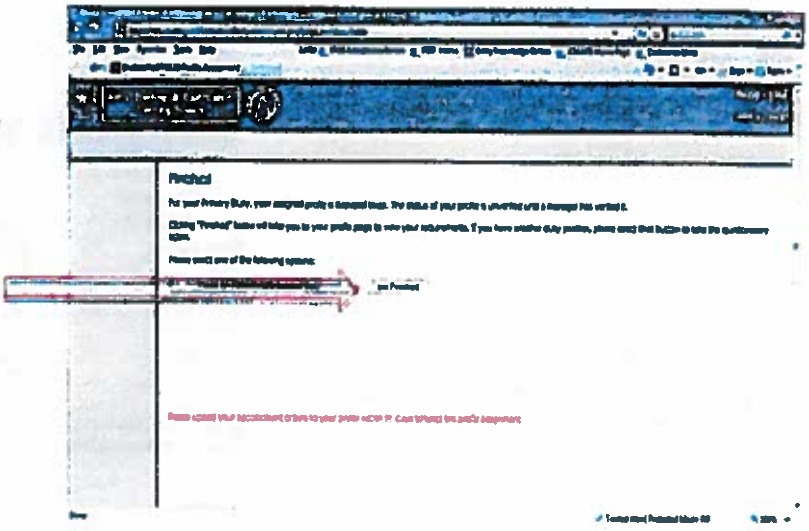
12 Click on " Proceed with CAC Login "

Questionnaire page opens.



13 Select which best describes your required access.

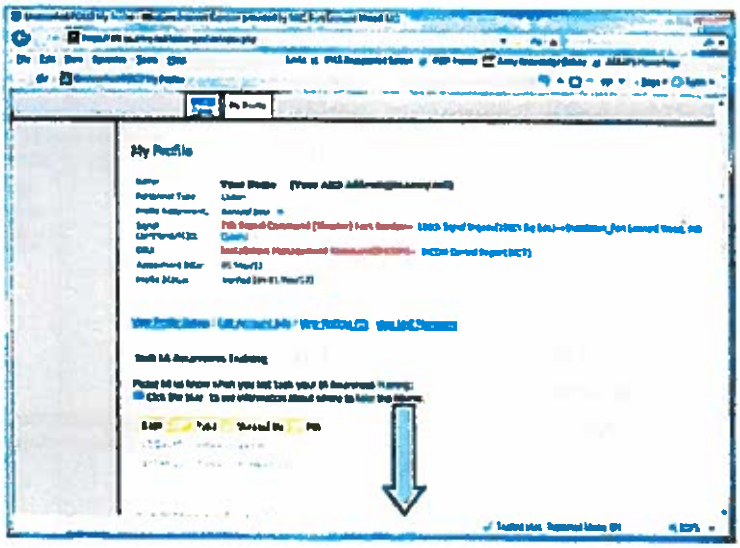
Finished notification page opens.



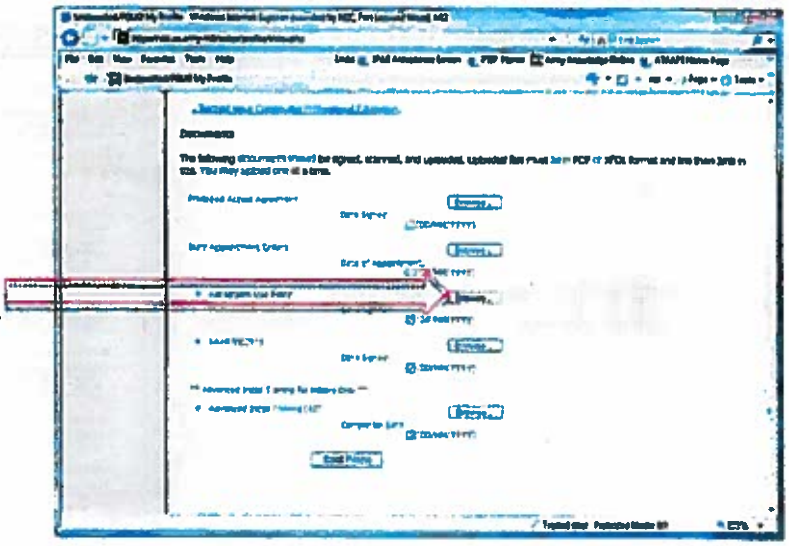
14 Click on " I am Finished " button.

My Profile page opens.

SCROLL Down



15 Click on " Browse " button to the Right of [?] Acceptable Use Policy.

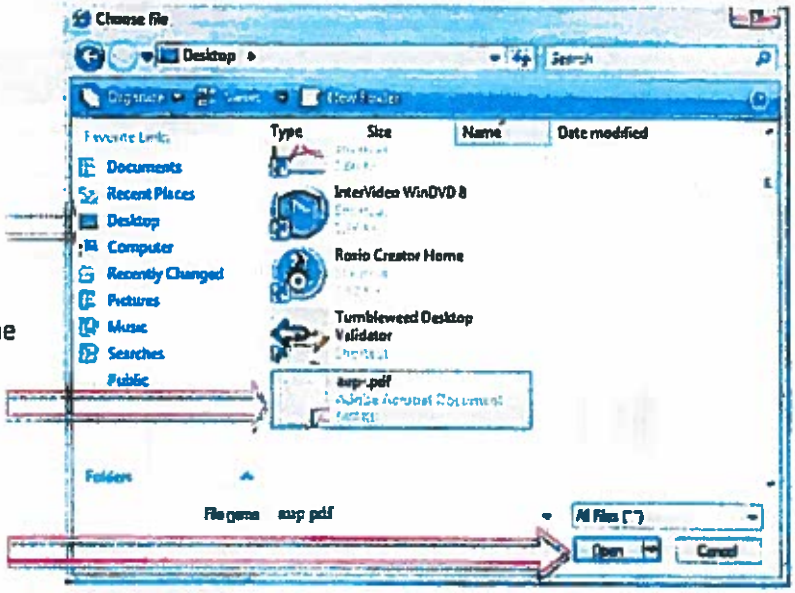


Choose File window opens.

16 Click Desktop in Favorite Links column.

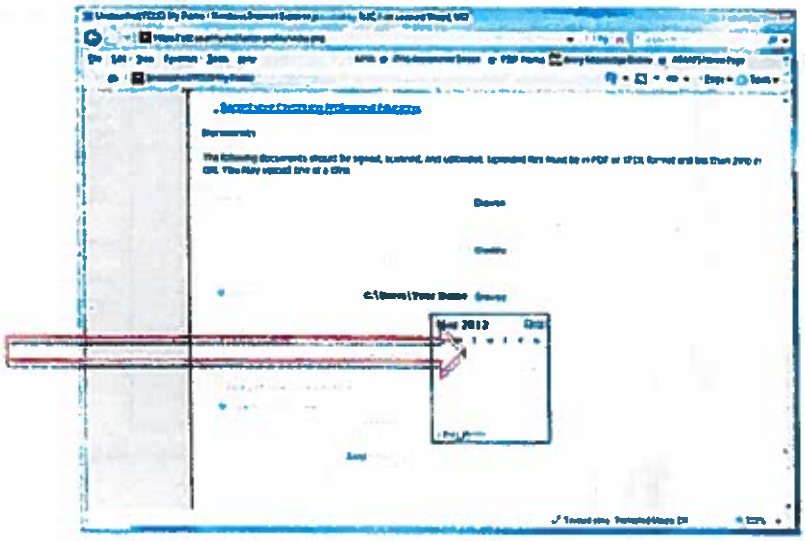
17 Find the file (AUP) you saved to the desktop in the column to the right and click on it.

18 Click on the " Open " button.



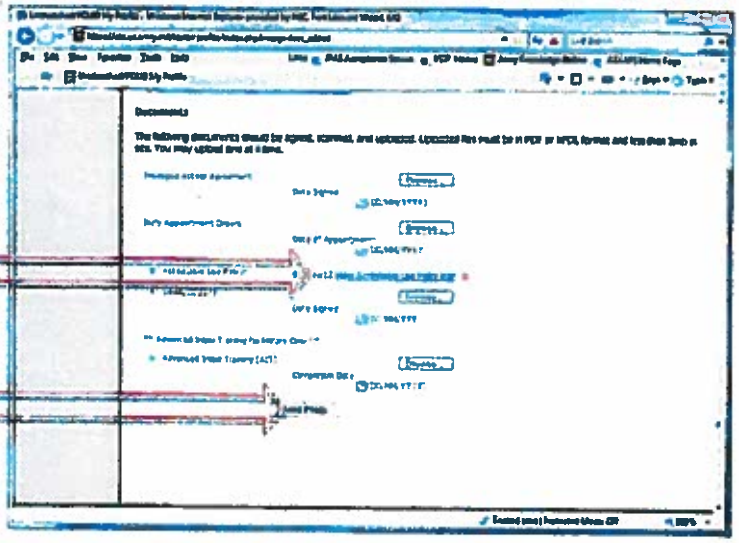
Return to the Documents section.

19 Click on the calendar icon to to open the calendar. Click on today's date.



If both selections are properly input then

you shall see View Accentable Use Policy PDF



20 Click on Send File(s) button.

21 Click " log out " link found top right Of web page.

Successful log out page opens.

NOTE: Upon successful log out you may either delete the AUP PDF you saved to the desktop or you can save it to another folder. The AUP is no longer needed.

Fort Leonard Wood Installation Camus Area Network Acceptable Use Policy Addendum

As a Fort Leonard Wood ICAN user I am tasked with the physical and operational security of any mobile device I utilize. I understand the following responsibilities if I utilize:

Remote access.

a. Remote Access will be via virtual private network (VPN).

b. Government owned hardware and software will be used.

c. The employee is the only individual authorized to use this equipment.

d. Access will be as authorized by the supervisor.

e. Requirements as indicated throughout this AUP are applicable for access to USG resources.

f. I will maintain the machines model, serial number, computer name and emergency point of contact information separately from the mobile computing device (MCD) while traveling.

g. I will secure the MCD at all times when not in use.

h. I will avoid using MCD's in an area where shoulder surfing is easy.

i. I will follow all information contained in IA BBP 06-EC-O-0007, Road Warrior Laptop Security, (https://informationassurance.us.army.mil).

j. While away from the installation I will ensure the MCD is connected to the FLW ICAN at least once a week via VPN. This connection will be maintained long enough to ensure required updates and patches are received.

k. In the event of any security incident (e.g., a classified spillage, loss of device, loss of personally identified information, etc.), I will contact my information assurance security officer (IASO) and NEC immediately and follow all FLW NEC Incident Response procedures.

l. I will always log off and shut down the MCD while in transit and not use sleep or hibernation mode.

m. I will utilize the MCD as a general user and will not attempt to install, reconfigure or disable any software. All MCD's will be maintained by the FLW NEC.

Blackberry devices.

a. I will be held responsible for damage caused to a Government system or data through negligence or a willful act.

b. I am not authorized and will not use Bluetooth technology with Blackberry devices except for the authorized products found on the Army approved two way wireless email device listing.

c. I will not operate a wireless device in areas where classified information is electronically stored or processed.

d. I will ensure the Blackberry handheld device is cradled or synced at least once every 30days to the Blackberry Enterprise Server (BES) to receive updated keys and/or software updates.

e. I understand that all charges incurred in excess of the normal monthly service charge (i.e. Additional per-minute charges, messaging, downloading features, neglect/abuse, games, subscriptions) will be the responsibility of the Blackberry user.

f. I have completed wireless training athttp://iatraining.disa.mil/eta/smartphone_tablet_v2/launchpage.htm

g. I understand that I must immediately notify appropriate site contacts (e.g. IASO, BES administrator, supervisor, etc.) if my BlackBerry is lost or stolen.

h. I will conform to all Army and DOD password and passcode standards.

i. When sending sensitive but unclassified and For Official Use Only information, emails should be encrypted or not sent.

j. I will treat any message or contact received from an unknown number or device with suspicion.

k. In the event of any security incident (e.g., a classified spillage, loss of personally identified information, etc.), I will contact my information assurance security officer (IASO) and NEC immediately and follow all FLW NEC Incident Response procedures.

l. I will be aware of my environment when using the Blackberry to prevent eavesdropping and shoulder surfing.

m. If mobile device email signatures are used, the signature message shall not disclose the email originated from a mobile device (e.g., "Sent From My BlackBerry Wireless Handheld").

n. The owner information setting will not have the organization's name or any information showing that the device is owned by the military.

I am aware of the following risks when utilizing the SMS service on a Blackberry device:

a. Messages are not encrypted and copies are stored in memory on the phone and in the wireless carrier database. Sensitive information will not be sent via SMS/Text/Messages/Multimedia Messaging Service (MMS).

b. URL to hacker web sites can be sent to a SMS/Text Message/MMS. If a user connects to the URL, malware could be downloaded on the phone.

c. Executable files (including malware) can be embedded in SMS/Text Message/MMS.

d. Photos sent via SMS/Text Messages/MMS can have URLs to hacker web sites embedded in the photo. When the photo is viewed the phone will connect to web site of the embedded web site.

e. Photos sent via SMS/Text Messages/MMS can have executable files (including malware) embedded in the photo. When the photo is viewed the phone will execute the file.

Wireless LAN

a. The use of wireless networks on the Fort Leonard Wood ICAN must be approved by the installation NEC prior to purchase and implementation of any products.

b. Any approved use of wireless networks must be implemented according to the Army's Wireless Security Standards BBP, 09-EC-M-0010 and will be implemented only with those products on the Unified Capabilities Approved Products List.

c. The connection of any wireless access points (WAPs) to the ICAN is strictly prohibited without prior approval from the installation NEC.

d. Any WAPs found on the network are subject to immediate confiscation by the installation NEC. The installation NEC will work with the command to determine proper disposal of confiscated WAP hardware.

e. I will remember that accessing the FLW ICAN via WLAN is no different than accessing via the wired network. All network rules and regulations still apply.

User signature and Date

DoD Information Assurance (IA) Awareness Training

The Army requires that all authorized users of DoD Information Systems receive Information Assurance (IA) awareness training as a condition to have network access. The Command/Directorate IASOs and the DOIM IA office identifies, tracks, and manages IA training compliance for annual DoD Federal Information Security Management Act (FISMA) reporting. Therefore, ALL FLW personnel with network accounts (military, government civilians, and contractors); will receive an email countdown for 14 days reminding them of their initial/renewal awareness training requirement. Users must take the **DoD Information Assurance Awareness** online training at the Fort Gordon website.

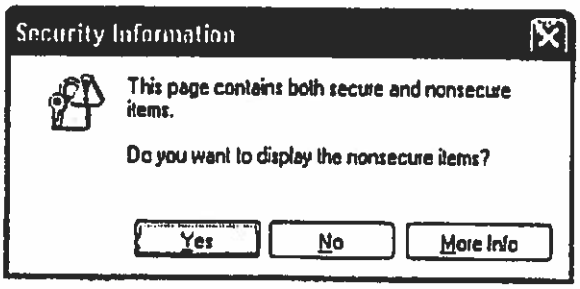
> **IMPORTANT: To meet mandatory Army IA training requirements, you must complete the DoD Information Assurance Awareness training and achieve a 70% or higher score to receive the DoD IA Awareness certificate signed from the Director, Fort Gordon School of Information Technology, DA Form 87.**

Please follow the instructions below to complete the mandatory DoD Information Assurance Awareness training:

A welcome message will be displayed from the U.S. Army Signal Center, Fort Gordon, GA https://ia.signal.army.mil/.

Follow the mandated IA Training "click here" link and on the next screen select the Annual DoD Information Assurance Awareness Training.

A Security Information Pop Up will appear, click "Yes" to allow nonsecure items. Then follow the steps in sequence:



- Select Step1 – DoDIAA Training
- Select Step 2 – Army Addendum, which provides answers to the exam questions in relation to Army requirements (since pop-ups are blocked select to "temporarily allow pop-ups" and/or "download file" and click "Yes" again on the allow nonsecure items).
- Select Step 3 – DoDIAA Exam

Last Step – After successfully completing the DoDIAA exam you may view and print the DoD Information Assurance Awareness certificate DA Form 87, signed by the Director, Fort Gordon School of Information Technology.

IMPORTANT NOTE FROM THE IA OFFICE:

You must provide the signed DoD IA Awareness training DA Form 87 certificate to your unit Information Assurance Security Officer (IASO). IASOs are encouraged to maintain hardcopy certificates for inspection purposes. IASOs will update the User Management System (UMS) database by revising the user's IAA training date and uploading the certificate.
If the database is not updated before the account expiration date, the account will be automatically disabled.

CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT

AN AGREEMENT BETWEEN AND THE UNITED STATES

(Name of Individual - Printed or typed)

1. Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to classified information. As used in this Agreement, classified information is marked or unmarked classified information, including oral communications, that is classified under the standards of Executive Order 13526, or under any other Executive order or statute that prohibits the unauthorized disclosure of information in the interest of national security; and unclassified information that meets the standards for classification and is in the process of a classification determination as provided in sections 1.1, 1.2, 1.3 and 1.4(e) of Executive Order 13526, or under any other Executive order or statute that requires protection for such information in the interest of national security. I understand and accept that by being granted access to classified information, special confidence and trust shall be placed in me by the United States Government.

2. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of classified information, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information have been approved for access to it, and that I understand these procedures.

3. I have been advised that the unauthorized disclosure, unauthorized retention, or negligent handling of classified information by me could cause damage or irreparable injury to the United States or could be used to advantage by a foreign nation. I hereby agree that I will never divulge classified information to anyone unless: (a) I have officially verified that the recipient has been properly authorized by the United States Government to receive it; or (b) I have been given prior written notice of authorization from the United States Government Department or Agency (hereinafter Department or Agency) responsible for the classification of information or last granting me a security clearance that such disclosure is permitted. I understand that if I am uncertain about the classification status of information, I am required to confirm from an authorized official that the information is unclassified before I may disclose it, except to a person as provided in (a) or (b), above. I further understand that I am obligated to comply with laws and regulations that prohibit the unauthorized disclosure of classified information.

4. I have been advised that any breach of this Agreement may result in the termination of any security clearances I hold; removal from any position of special confidence and trust requiring such clearances; or termination of my employment or other relationships with the Departments or Agencies that granted my security clearance or clearances. In addition, I have been advised that any unauthorized disclosure of classified information by me may constitute a violation, or violations, of United States criminal laws, including the provisions of sections 641, 793, 794, 798, *952 and 1924, title 18, United States Code; *the provisions of section 783(b), title 50, United States Code; and the provisions of the Intelligence Identities Protection Act of 1982. I recognize that nothing in this Agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation.

5. I hereby assign to the United States Government all royalties, remunerations, and emoluments that have resulted, will result or may result from any disclosure, publication, or revelation of classified information not consistent with the terms of this Agreement.

6. I understand that the United States Government may seek any remedy available to it to enforce this Agreement including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement.

7. I understand that all classified information to which I have access or may obtain access by signing this Agreement is now and will remain the property of, or under the control of the United States Government unless and until otherwise determined by an authorized official or final ruling of a court of law. I agree that I shall return all classified materials which have, or may come into my possession or for which I am responsible because of such access: (a) upon demand by an authorized representative of the United States Government; (b) upon the conclusion of my employment or other relationship with the Department or Agency that last granted me a security clearance or that provided me access to classified information; or (c) upon the conclusion of my employment or other relationship that requires access to classified information. If I do not return such materials upon request, I understand that this may be a violation of sections 793 and/or 1924, title 18, United States Code, a United States criminal law.

8. Unless and until I am released in writing by an authorized representative of the United States Government, I understand that all conditions and obligations imposed upon me by this Agreement apply during the time I am granted access to classified information, and at all times thereafter.

9. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions of this Agreement shall remain in full force and effect.

10. These provisions are consistent with and do not supersede, conflict with, or otherwise alter the employee obligations, rights, or liabilities created by existing statute or Executive order relating to (1) classified information, (2) communications to Congress, (3) the reporting to an Inspector General of a violation of any law, rule, or regulation, or mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety, or (4) any other whistleblower protection. The definitions, requirements, obligations, rights, sanctions, and liabilities created by controlling Executive orders and statutory provisions are incorporated into this agreement and are controlling.

(Continue on reverse.)

11. These restrictions are consistent with and do not supersede, conflict with, or otherwise alter the employee obligations, rights, or liabilities created by Executive Order No. 13526 (75 Fed. Reg. 707), or any successor thereto section 7211 of title 5, United States Code (governing disclosures to Congress); section 1034 of title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military); section 2302(b) (8) of title 5, United States Code, as amended by the Whistleblower Protection Act of 1989 (governing disclosures of illegality, waste, fraud , abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 U.S.C. 421 et seq.) (governing disclosures that could expose confidential Government agents); sections 7(c) and 8H of the Inspector General Act of 1978 (5 U.S.C. App.) (relating to disclosures to an inspector general, the inspectors general of the Intelligence Community. and Congress); section 103H(g)(3) of the National Security Act of 1947 (50 U.S.C. 403-3h(g)(3) (relating to disclosures to the inspector general of the Intelligence Community); sections 17(d)(5) and 17(e)(3) of the Central Intelligence Agency Act of 1949 (50 U.S.C. 403g(d)(5) and 403q(e)(3)) (relating to disclosures to the Inspector General of the Central Intelligence Agency and Congress); and the statutes which protect against disclosure that may compromise the national security, including sections 641, 793, 794, 798, *952 and 1924 of title 18, United States Code, and *section 4 (b) of the Subversive Activities Control Act of 1950 (50 U.S.C. section 783(b)). The definitions, requirements, obligations, rights, sanctions, and liabilities created by said Executive Order and listed statutes are incorporated into this agreement and are controlling.

12. I have read this Agreement carefully and my questions, if any, have been answered. I acknowledge that the briefing officer has made available to me the Executive Order and statutes referenced in this agreement and its implementing regulation (32 CFR Part 2001 , section 2001 .80(d)(2)) so that I may read them at this time, if I so choose.

* NOT APPLICABLE TO NON-GOVERNMENT PERSONNEL SIGNING THIS AGREEMENT.

SIGNATURE	DATE	SOCIAL SECURITY NUMBER *(See Notice below)*

ORGANIZATION (IF CONTRACTOR, LICENSEE, GRANTEE OR AGENT, PROVIDE NAME, ADDRESS, AND, IF APPLICABLE, FEDERAL SUPPLY CODE NUMBER) *(Type or print)*

WITNESS		ACCEPTANCE	
THE EXECUTION OF THIS AGREEMENT WAS WITNESSED BY THE UNDERSIGNED.		THE UNDERSIGNED ACCEPTED THIS AGREEMENT ON BEHALF OF THE UNITED STATES GOVERNMENT.	
SIGNATURE	DATE	SIGNATURE	DATE
NAME AND ADDRESS *(Type or print)*		NAME AND ADDRESS *(Type or print)*	

SECURITY DEBRIEFING ACKNOWLEDGEMENT

I reaffirm that the provisions of the espionage laws, other federal criminal laws and executive orders applicable to the safeguarding of classified information have been made available to me; that I have returned all classified information in my custody; that I will not communicate or transmit classified information to any unauthorized person or organization; that I will promptly report to the Federal Bureau of Investigation any attempt by an unauthorized person to solicit classified information, and that I (have) (have not) (strike out inappropriate word or words) received a security debriefing.

SIGNATURE OF EMPLOYEE	DATE

NAME OF WITNESS *(Type or print)*	SIGNATURE OF WITNESS

NOTICE: The Privacy Act, 5 U.S.C. 552a, requires that federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that authority for soliciting your Social Security Number (SSN) is Public Law 104-134 (April 26, 1996). Your SSN will be used to identify you precisely when it is necessary to certify that you have access to the information indicated above or to determine that your access to the information indicated has been terminated. Furnishing your Social Security Number, as well as other data, is voluntary, but failure to do so may delay or prevent you being granted access to classified information.

HQs TRADOC
Fort Eustis, VA
14 AUG 12

Annex B (OPSEC Measures) to TRADOC OPSEC Plan 12-004

1. Personnel will abide by the following OPSEC measures:

a. General measures to protect critical or sensitive information. Critical or sensitive information includes For Official Use Only (FOUO), information protected by the Freedom of Information Act, Essential Elements of Friendly Information (EEFI) or Critical Information List (CIL), Personally Identifiable Information (PII), and information protected by the Privacy Act of 1974 as well as information covered by the Health Insurance Portability and Accountability Act (HIPAA).

(1) Critical or sensitive information must be encrypted when disseminated via e-mail within Army information systems.

(2) When disposing of critical or sensitive information, shred, burn, or destroy per local policy. DO NOT discard in trash or recycle bins. Do not allow paper recycle bins in secure or sensitive areas.

(3) Avoid open posting of schedules that reveal when sensitive events will occur.

(4) Control the issuance of orders, movement of units, programs, or key personnel lists.

(5) Protect sensitive unclassified information by at least one physical or electronic barrier (e.g., locked container or room, logical authentication or logon procedure) when not under direct individual control of an authorized user.

(6) Ensure that government conversations, web postings, blogs, social media comments, or releases to the media and/or public receive appropriate OPSEC reviews prior to being disclosed or transmitted. See Annex F.

(7) Do not wear security badge(s) outside secure areas. Avoid allowing pictures to be taken of security badge(s) and/or other sensitive information.

(8) Limit release of sensitive information until latest possible date or until those events are complete

b. Conference and Meeting security measures.

(1) Conduct meetings, briefings and conferences in locations authorized and appropriate to the level and classification of information discussed at the location. Classified meetings will only be held at appropriately cleared U.S. Government or U.S. Government contractor facilities. Classified meetings in public facilities are prohibited. Meetings of 300 or more require a threat assessment.

(2) Before starting the meeting, the meeting coordinator will inspect the location and adjacent areas to ensure unauthorized personnel cannot monitor.

(3) The meeting coordinator will secure the area until a cleared person in charge of the meeting opens the room to attendees. The individuals responsible for arranging the meeting are responsible for security of the meeting. The responsible individual will:

(a) Notify the attendees of the classification or sensitivity of the meeting.

(b) Prepare the room for classified or sensitive discussion. Clear adjacent rooms, turn off audio/video equipment not needed for the briefing, and ensure attendees have no cellular phones or communication devices during classified briefings.

(c) Ensure each person attending the meeting has the appropriate access authorization.

(d) Control ingress and egress to the room during discussions and after each break.

(e) Ensure that notes taken during the meeting are properly marked, handled, collected, maintained by authorized personnel and/or destroyed afterwards.

(f) Ensure that adequate storage facilities are available for classified or sensitive information, when required.

(g) Inspect the conference room immediately after the meeting to ensure no sensitive information has been left behind.

(h) Avoid allowing sensitive information and security badges to be photographed or copied.

c. Employee travel measures.

(1) Travel in civilian clothes whenever possible. Do not carry luggage, including briefcases, which identifies you as a member of the command.

(2) Use a passport or other ID instead of military orders whenever possible.

(3) Do not discuss assignments, duties, or reason for travel unless absolutely necessary (e.g., with security, customs, or immigration personnel).

(4) Do not use public or personal computers for Government business. If you use a public computer for personal business, understand your passwords and personal data are at risk of compromise. When using public computers, be sure to log off all accounts, and clear history and cookies on exit.

d. Social Networking Site measures.

(1) Take a close look at all privacy settings. Set security options to allow visibility to "friends only."

(2) Do not reveal sensitive information about yourself such as mission schedules, briefings, and event locations. Ask, "What could the wrong person do with this information?" and "Could it compromise the safety of me, my family or my unit?"

(3) Geo-tagging is a feature that reveals your location to other people within your network. Consider turning off the GPS function of your smart phone in all appropriate circumstances.

(4) Closely review all Army related photos before they go online. Make sure they do not give away sensitive information which could be dangerous if released. (For example, photos of your unit on a mission, sensitive equipment or areas, documents, briefing slides, security, badges, etc, and what is exposed in the background?)

(5) Make sure to talk to family about operations security and what can and cannot be posted or discussed. Avoid disclosure of unnecessary potentially sensitive information outside the work place.

(6) Videos can go viral quickly; make sure they don't give away sensitive information.

(7) Avoid mentioning rank, unit locations, deployment dates, names, or equipment specifications and capabilities.

(8) If you would not want it made public, do not post it.

e. Visitor Control and Personnel Security.

(1) Establish a visitor control system to coordinate and control all visits.

(2) Provide escorts for visitors and vendors who need access to restricted areas.

(3) Ensure escorts know proper escort procedures, limitations of disclosure, and other applicable controls involved in the visit.

f. Communications Security measures.

(1) Do not discuss or transmit sensitive information over wireless unsecure devices such cell phones, computer data networks, or Bluetooth.

(2) When discussing sensitive or critical information, make maximum use of secure communications. All e-mails sent must be encrypted if they contain sensitive or critical information.

(3) Limit reading file distribution to personnel with need to know. Control distribution of non-classified, sensitive information in accordance with distribution markings for technical and operational information (FOUO, CUI, Restricted, etc).

(4) Enforce strict compliance with command information systems policies on the use of all computer systems.

(5) Limit mission-related email to only official DoD accounts.

(6) Log off computer or remove CAC card when away from work area.

(7) Prohibit unauthorized hardware or software on Army systems.

(8) Limit use of personally owned devices, to include mobile devices, to only those documents that are approved for public release. Do not download FOUO or other distribution restricted documents and files to your personally owned devices. This includes emailing the documents and files to a commercially owned email account.

(9) Do not process DoD information on publically available computers (e.g., those available for use by the general public in kiosks or hotel business centers).

(10) Encrypt wireless connections and use encrypted wireless connections where available when traveling (VPN, etc).

(11) Transmit voice and fax transmissions only when there is a reasonable assurance that access is limited to authorized recipients.

(12) Do not post sensitive information to website pages that are publicly available or have access limited only by domain or Internet protocol restriction. Such information may be posted to website pages that control access by DoD PKI certificates, or other technical means and provide protection.

2. POC for this Annex is TRADOC OPSEC Officer, David Speigner, (757) 501-5107, david.speigner@us.army.mil.

TRADOC Operations Security (OPSEC) Individual User Compliance Agreement

Operations Security (OPSEC) is a key protection element that protects the Warfighter, our Army, our families, and all the personnel that support their efforts. OPSEC relies on every individual understanding what critical information is, and knowing how to protect it. It is incumbent on every person to do their part, and practice good OPSEC. Through your efforts, you can help prevent release of sensitive information that may lead to serious injury or death to personnel, damage to weapons systems, equipment, facilities, loss of sensitive technologies, and mission failure.

1. I know my critical information. Critical or sensitive information includes For Official Use Only (FOUO), information, Essential Elements of Friendly Information (EEFI) or Critical Information List (CIL), Personally Identifiable Information (PII), and information protected by the Privacy Act of 1974 as well as information covered by the Health Insurance Portability and Accountability Act (HIPAA).

I have read and understand Annex B to the TRADOC OPSEC Plan, and my unit's EEFI or CIL.

2. I know how to protect my critical information.

I will ensure waste containing critical or sensitive information is destroyed in a manner to prevent disclosure (e.g. shredded or burned per local policy).

I will never discard critical or sensitive information in a trash or recycle bin.

I will ensure that government conversations, web postings, blogs, social media comments, or releases to the media and/or public receive appropriate OPSEC reviews prior to being disclosed, posted or transmitted.

I will not display my security badge(s) outside secure areas. I will avoid allowing pictures to be taken of my security badge(s) and/or other sensitive information.

I will talk to my family about OPSEC and the need and obligation to protect critical information.

I will not discuss or transmit sensitive information over wireless unsecure devices.

I will encrypt all e-mails that contain sensitive or critical information.

I will limit mission-related e-mail traffic to only official DoD accounts.

I will limit use of personally owned devices to only those documents that are approved for public release.

I will not process DoD information on public computers (e.g., those available for use by the general public in kiosks, libraries, or hotel business centers).

When traveling, I will use encrypted connections where available (VPN, etc), and I will secure my media and documents at all times.

Acknowledgement of Responsibilities: Personnel who fail to comply with orders, directives, or policies to protect critical and sensitive information may be punished under violations of a lawful order under UCMJ, Art. 92 or under other disciplinary, administrative, or other actions as applicable. Personnel not subject to the UCMJ who fail to protect critical and sensitive information from unauthorized disclosure may be subject to administrative, disciplinary, contractual, or criminal action. I acknowledge.

_____ _____

Signature Date

_____

Printed Name

U.S. ARMY TRAINING AND DOCTRINE COMMAND
NORTH ATLANTIC TREATY ORGANIZATION (NATO)
SECURITY BRIEFING

FOREWORD

This security briefing contains the minimum elements of information that must be provided to individuals upon initial indoctrination for access to NATO classified information.

This briefing is intentionally general so it may be used by all U.S. Government agencies and contractors. Agencies and contractors are encouraged to expand upon this briefing to accommodate specific situations. There is no requirement to copy this format or literary style; however, the minimum elements contained herein shall be included. Detailed procedures are contained in United States National Security Authority for NATO (USSAN) Instruction 1-07, NATO's C-M(2002) 49 "Security within The North Atlantic Treaty Organization" and its Supporting Security Directives (AC/35-D/2000 through D/2005), and the National Industrial Security Program Operating Manual (NISPOM) DoD 5220.22-M.

INTRODUCTION

You will require access to NATO classified information in pursuance of your current duties. The security standards and procedures for handling and protecting NATO information are in some cases different than those for U.S. information. This briefing explains the basic security standards and procedures for safeguarding NATO information.

WHAT IS NATO?

NATO is an acronym for the North Atlantic Treaty Organization. Member nations have signed the North Atlantic Treaty and the NATO Security Agreement, which obligate them to comply with NATO rules. The following nations are members of NATO:

Belgium	Hungary	Portugal	Turkey	Bulgaria	Slovenia
Canada	Italy	Spain	Norway	Estonia	Albania
Czech Republic	Luxembourg	United Kingdom	Iceland	Latvia	Croatia
Germany	Netherlands	United States	France	Lithuania	
Greece	Poland	Denmark	Romania	Slovakia	

The Secretary of Defense is the United States National Security Authority for NATO. As such, he is responsible for ensuring that NATO security requirements are implemented throughout the Executive Branch of the United States Government.

WHAT IS NATO INFORMATION?

NATO information is information that has been generated by or for NATO, or member nation national information that has been released into the NATO security system. The protection of this information is controlled under the NATO security regulations, and access within NATO is determined by the holder, unless restrictions are specified by the originator at the time of release to NATO.

Material received by an agency direct from another NATO member nation may contain either NATO information generated by a NATO element or national information generated by a NATO member nation. If it has been marked "NATO" by the originating nation, it must be assumed to contain information released to NATO, and it is controlled under the NATO Security Program.

If the material has a national classification marking and is not marked "NATO" by the originator, DO NOT apply a NATO marking unless you are informed in writing by the originator that the material is intended for NATO and is to be protected under the NATO Security Program. Moreover, the material or the information therein shall not be released into the NATO system without the prior written consent of the originator.

"RELEASABLE TO NATO" statements on U.S. material indicate that the information contained therein has been authorized under applicable disclosure policies for release to NATO and may be discussed within the NATO community. ONLY the copies that are being released to NATO shall be marked with a NATO marking. They are to be dispatched and controlled in the NATO registry system or in accordance with guidance provided by the supporting sub-registry or control point. The remaining copies shall continue to be controlled as U.S. information. There must be a record, however, that the information has been authorized for release to NATO.

CLASSIFICATION MARKINGS AND CATEGORIES OF NATO INFORMATION

NATO has four levels of classified information: COSMIC TOP SECRET, NATO SECRET, NATO CONFIDENTIAL, and NATO RESTRICTED. Certain NATO information is further classified in a specific category as ATOMAL which can be either RESTRICTED DATA (RD) or FORMERLY RESTRICRED DATA (FRD). NATO also distinguishes official, unclassified information. The markings and categories of NATO information are described below.

****NOTE: U.S. Army Training and Doctrine Command (TRADOC) NATO Control Points and User Agencies are authorized access to NATO Secret and below only. Access to COSMIC and ATOMAL information is not authorized.****

COSMIC TOP SECRET (CTS) - This security classification is applied to information the unauthorized disclosure of which would cause exceptionally grave damage to NATO. (NOTE: The marking "COSMIC" is applied to TOP SECRET material to signify that it is the property of NATO. The term "NATO TOP SECRET" is not used.)

NATO SECRET (NS) - This security classification is applied to information the unauthorized disclosure of which would cause serious damage to NATO.

NATO CONFIDENTIAL (NC) - This security classification is applied to information the unauthorized disclosure of which would be damaging to the interests of NATO.

NATO RESTRICTED (NR) - This security classification is applied to information the unauthorized disclosure of which would be disadvantageous to the interests of NATO. (NOTE: Although the security safeguards for NATO RESTRICTED material are similar to those of FOR OFFICIAL USE ONLY, OFFICIAL USE ONLY, or SENSITIVE, BUT UNCLASSIFIED information, "NATO RESTRICTED" is a security classification.)

ATOMAL - ATOMAL information can be either U.S. Restricted Data or Formerly Restricted Data that is classified pursuant to the Atomic Energy Act of 1954, as amended, or United Kingdom ATOMIC information that has been officially released to NATO. ATOMAL information is marked either COSMIC TOP SECRET ATOMAL (CTSA), NATO SECRET ATOMAL (NSA).

NATO UNCLASSIFIED (NU) - This marking is applied to official information that is the property of NATO, but does not meet the criteria for classification. Access to the information by non-NATO entities is permitted when such access would not be detrimental to NATO. In this regard, it is similar to U.S. Government official information that must be reviewed prior to public release.
(As of mid-2002, NATO has required its classified information to be portion-marked, i.e. with a classification marking applied to each paragraph heading, etc.)

ACCESS AUTHORIZATION

NATO Classified Information. As with U.S. information, access is NOT based on duty position, rank, or level of clearance. Access is based on need-to-know, the proper level of U.S. clearance, and an access briefing for a specific level and type of NATO/ATOMAL information.

Remember, it is your responsibility to ensure that an individual is authorized access to a particular type and level of classified NATO or/and ATOMAL information BEFORE you provide access. This responsibility applies to all modes of transmission, e.g., oral, written, visual and electronic. If in doubt, seek assistance from your

security officer or NATO sub-registry or control point. NATO information is provided to non-NATO nationals and entities only with the approval of the originator of the information. That approval is gained through the appropriate NATO committee.

THE REGISTRY SYSTEM

A Central Registry has been established by each NATO member nation to ensure proper control and accountability of NATO classified documents. The Central United States Registry (CUSR) is located in Arlington, Virginia. As an official representative of the U.S. Security Authority for NATO, the CUSR oversees the administration of the U.S. registry system. The CUSR establishes all U.S. sub-registries to execute the accountability and security management of NATO and ATOMAL material at various U.S. locations throughout the world. Based on location and volume of material, control points may be established to assist in these operations.

ACCOUNTING FOR NATO CLASSIFIED MATERIAL

COSMIC TOP SECRET, NATO SECRET, and all ATOMAL. Receipts and logs shall be maintained on the receipt, disposition, destruction, and dispatch of COSMIC TOP SECRET, NATO SECRET, and all ATOMAL material. In addition, each individual is required to execute a disclosure record upon acquiring access to each item of CTS/CTSA material, or ATOMAL with special limitation restrictions.

NATO CONFIDENTIAL and NATO RESTRICTED. You are required to maintain administrative control of NATO CONFIDENTIAL and NATO RESTRICTED material adequate to preclude unauthorized access. Specific accounting records are not necessary unless they are required by the originator.

MARKING AND ACCOUNTING FOR U.S. DOCUMENTS CONTAINING NATO CLASSIFIED INFORMATION

A newly generated U.S. classified document that contains NATO classified information shall bear a U.S. classification marking that reflects the highest level of NATO or U.S. classified information it contains. Declassification and downgrading instructions shall indicate that the NATO information is exempt from downgrading or declassification without the prior consent of NATO; the reason to be cited is "foreign government information."

The statement "THIS DOCUMENT CONTAINS NATO CLASSIFIED INFORMATION" will be affixed to the front cover or first page, if there is no cover. Portions that contain NATO classified information shall be marked to identify the information (e.g., NS). The document shall be accounted for, safeguarded and controlled as specified for NATO documents of the same classification.

If a record is required for the NATO classification information, a U.S. document containing the NATO information will be logged, accounted for and handled in the same manner as required for the NATO information. However, NATO reference numbers are not required. A record shall be maintained of source NATO documents, as required for derivatively classified U.S. documents.

Existing U.S. documents that do not meet this requirement shall be marked and handled according to these procedures when they are removed from the files for use.

AIS storage media shall be handled as described in C-M(2002)49, its Supporting Directives, and USSAN 1-07, Section 7, Page 31)

SAFEGUARDING NATO MATERIAL

General. The physical security requirements for material marked NATO CONFIDENTIAL and above are the same as for U.S. material of the same level of classification. NATO RESTRICTED material may be stored in a locked filing cabinet, book case, desk or other such container, or in a room or building that is locked during non-duty hours, provided access to the room or building is controlled so that only authorized personnel can gain access to the information. All personnel with access to a security container that is used to store NATO information must be briefed and authorized access to the level and type of NATO information that is stored in that container.

Segregation. You are required to ensure that NATO and non-NATO material are filed separately. ATOMAL material must be filed separately from non-ATOMAL material. This may be accomplished by using a separate security container or, to conserve storage space, by using separate drawers or file dividers in the same security container holding U.S. classified material. Additionally, you are required to segregate ATOMAL control records from non-ATOMAL control records.

Combinations. Combinations to security containers containing NATO classified material must be changed at least annually, upon departure of an individual with access to the combination, or if the combination has been or is suspected of having been compromised.

Transmission. The national or international transmission of CTS and CTSA material shall be through the registry system using a cleared government courier service; for example, diplomatic pouch or military courier service. The national and international transmission of NS, NSA, NC, and NCA shall be by cleared courier, or by appropriately cleared and briefed employees who possess courier identification and authorization, or by U.S. registered mail using the same provisions as prescribed for U.S. classified material. Receipts are required for CTS, NS and all ATOMAL material. NC may also be sent by U.S. First Class mail between U.S. Government activities within the United States.

In urgent situations, the United States Postal Service Express Mail may be used to transmit material NS and below within the United States, its Territories, and the District of Columbia. However, there are restrictions on the use of Express Mail; guidance should be sought from your security officer or sub-registry or control point. NR material may be sent by U.S. First Class mail within the United States and to an APO/FPO or NATO address through the U.S. or NATO member nation postal service.

Automated Information Systems (AIS). Systems must be accredited specifically to handle NATO classified information. Organizations with AIS systems accredited for handling NATO classified information must issue instructions for processing, handling and accounting for NATO classified information. Be sure you receive a copy of those instructions and apply them. NATO accredited SIPRNET, JWICS, U.S. BICES, and CENTRIX-ISAF are the only authorized networks approved to transmit and store NATO SECRET information and below, to include NATO Unclassified.

Destruction. The destruction of CTS, CTSA, NS, and NSA material will be accomplished only by registry system personnel using a destruction certificate and a method approved for the destruction of U.S. material of the same level of classification. NATO CONFIDENTIAL, NATO RESTRICTED and NATO UNCLASSIFIED shall be destroyed by any means authorized for U.S. CONFIDENTIAL material.

Reproduction. COSMIC documents shall be reproduced by the Central US Registry and COSMIC Sub-registries which must report the number of copies made to the CUSR. Reproduction of ATOMAL (CTSA, and NSA) shall be made only by the CUSR, ATOMAL Subregistries and ATOMAL Control Points. Reproduction of NATO Secret and below may be produced by the addressee under strict need-to-know principle and provided that the originator has not restricted reproduction. Reproduced copies shall be accounted for and safeguarded in the same manner as the original.

SECURITY VIOLATIONS AND POSSIBLE LOSS/COMPROMISE OF NATO CLASSIFIED MATERIAL

General. NATO guidelines are very similar to those used for U.S. material. However, the servicing sub-registry or control point must be informed of the incident, in addition to the responsible security or counterintelligence officials.

Procedures. If you find NATO material unsecured and unattended, immediately contact your security officer or registry system official. Stay with the material and wait for the security officer or registry official to arrive. Do not disturb the area or material. Do not allow anyone else to disturb the area or allow unauthorized personnel to have access to the material.

If it is necessary that you leave the area before your security officer or registry system official can assume custody, place the material in a security container and lock the container. If the container is already locked, and you are not authorized access, or there is no container, take the material directly to an appropriately cleared security or registry system official, explain the circumstances, and obtain a receipt for the material.

Espionage, Sabotage, Terrorism, and Deliberate Compromise. Information concerning a deliberate compromise of NATO/ATOMAL material, attempted or actual espionage directed against NATO/ATOMAL information, or actual or planned terrorist or sabotage activity against facilities or users of NATO classified material shall be reported promptly to your security officer or to your agency's counterintelligence officer or the Federal Bureau of Investigation. The following are typical reportable situations:

1. Attempts by unauthorized persons to obtain classified information concerning NATO or U.S. facilities, activities, personnel, or material through questioning, elicitation, bribery, threats, or coercion, either by direct or indirect contacts or correspondence.

2. Attempts by unauthorized persons to obtain classified information through photographing, wiretapping, eavesdropping, observation, or by any other means.

3. Attempts by persons with known, suspected, or possible foreign intelligence backgrounds, associations, or activities to establish a friendship or a social or business relationship, or to place you under obligation through special treatment, favors, gifts, money, or other means.

4. Information concerning terrorist plans and activities posing a direct threat to U.S. or NATO facilities, activities, personnel or material.

5. Known or suspected acts or plots to harm or destroy U.S. or NATO property by sabotage.
Anyone with access to NATO classified information could be a potential target. If you become aware of activities such as those as described above, or someone approaches you directly to engage in such activities, remember the following:

a. STAY CALM. You are not at fault because they chose to target you.

b. BE NONCOMMITTAL. Be ambiguous as to whether or not you will provide them with material or information.

c. REPORT IT PROMPTLY. Even if it seems purely coincidental or insignificant, a small detail may be the key to identifying and countering espionage or sabotage or a terrorist act. Do not discuss the incident with friends, family, co-workers, etc., unless directed to by your security officer or counterintelligence representative.

d. IT IS NEVER TOO LATE! If you have provided material or information to an unauthorized recipient, report it.

FOREIGN TRAVEL

Your personal travel will not be limited based solely on the fact that you have access to NATO classified information. There are, however, risks involved in travel to certain countries. Check with your security officer for advice and assistance. If you choose to travel to high-risk countries, you are required to coordinate with your leave/travel order granting authority and security office and obtain a travel security briefing. Upon your return, you should report any incident that may have been an attempt to collect sensitive information.

WHERE DO I GO FOR MORE HELP?

If problems or specific questions arise concerning NATO information, your security officer or the HQ U.S. Army TRADOC NATO Secret Sub-Registry Officer can assist you.

Barth, Lisa L CIV (US)

From: Dodson, Beverly J CIV (US)
Sent: Friday, July 13, 2012 2:56 PM
To: Barth, Lisa L CIV (US)
Subject: Work Order 392183 - Closing (UNCLASSIFIED)
Attachments: Updating GAL (2).pptx

Classification: UNCLASSIFIED
Caveats: NONE

Ms. Barth,

Users can now go to http://milconnect.dmdc.mil to update their information, which will also update DEERS.

See attachment for step-by-step instructions.

Users can: 1) change email display name to show your nickname or middle name; 2) change email display to show the correct organization and 3) change/correct their phone number in the EE GAL.

Although the site is being updated to make it easier to use, the portal can sometimes be a little tricky/confusing right now, so a guide has been created that will walk you through making the updates you desire. It can be found at https://ee.csd.disa.mil. This site requires CAC authentication. The guide has information on both legacy active directory updates and Enterprise Email updates. For EE updates, start with paragraph #5 at the top of page 6.

Please call 3-HELP if you need additional assistance.

Sincerely,

NEC

Beverly Dodson

IT Specialist

Network Enterprise Center (NEC)

464 MANSCEN Loop, Ste 3641

Fort Leonard Wood, MO 65473

HYPERLINK "mailto:beverly.j.dodson3.civ@mail.mil"beverly.j.dodson3.civ@mail.mil

Classification: UNCLASSIFIED
Caveats: NONE

Per the attached e-mail sent from GEN John F Campbell, Vice Chief of Staff, Army, all Army personnel, yes AD, CIV and Contractors, must update their information in MilConnect. Please note, DISA Enterprise has already started suspending Enterprise E-mail accounts for failure to comply with this mandatory requirement.

You can either click on the FLW Helpful Links Folder on your desktop, then click on the MilConnect shortcut, or type in, https://www.dmdc.osd.mil/milconnect, log in with your CAC, go to the "My

Profile" tab, then "Update and View My Profile" from the drop down list, next select the "Mil"; "Civ" or "Ctr" tab and update all of your official information:

Personnel Status (**Use your organizational information**):

Duty Organization: United States Army

Duty Sub-organization: TRADOC Engineer School (this one is about an inch or so from the bottom of the list when you scroll down, it's way under the MEDCOM group)

Office Symbol: ATSE-...

Job Title: Whatever your title is

Duty Installation/Location: Fort Leonard Wood, MO

Building: 3201

Room: You can put a room number or your section

Addresses:

USAES, HQ

14010 MSCoE Loop

Bldg 3201, Ste 1661

Fort Leonard Wood

MO

65473

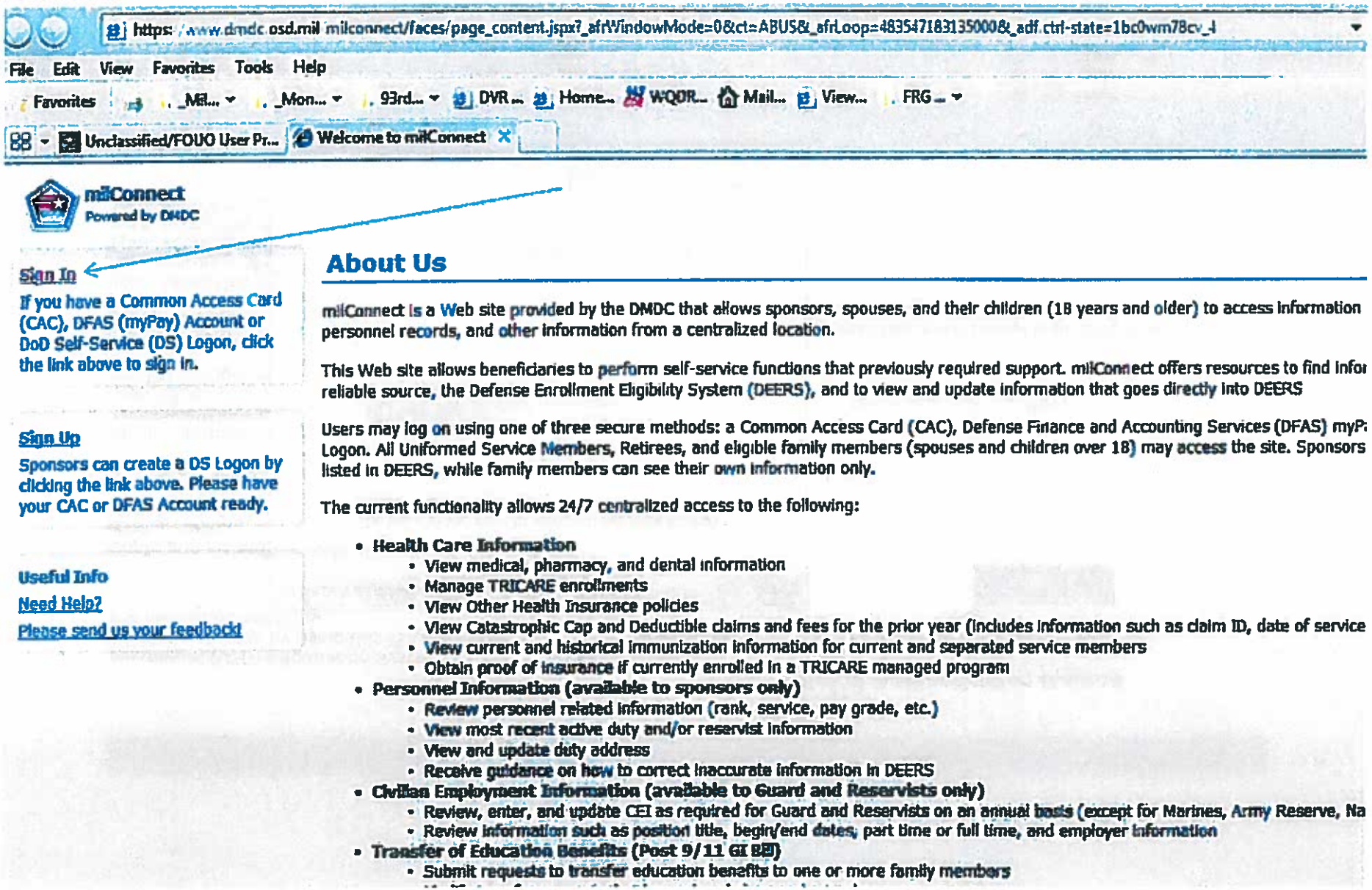
United States

Phone/Fax Numbers:

Duty: 573-596-XXXX or 0131 with extension, if it's not a direct dial number.

That's all the important information that needs to be update, if you choose to fill in all the other blanks, that's also your choice.

https://www.dmdc.osd.mil/milconnect/faces/page_content.jspx?_afrWindowMode=0&ct=ABUS&_afrLoop=483959837299000&_adf.ctrl-state=rwfwezv8v_4



overnment (USG) Information System (IS) that is provided for USG
horized use only. By using this IS (which includes any device attached
the following conditions:

rcepts and monito
etration testing, C
(PM), law enforcer

ıay inspect and se

tifying information
communications u
: subject to routin
ny USG authorize

y measures (e.g.,
personal benefit

bove, using this IS
or monitoring of
sonal representat
ants. Such commu
Agreement for det

t

Select Authentication Method

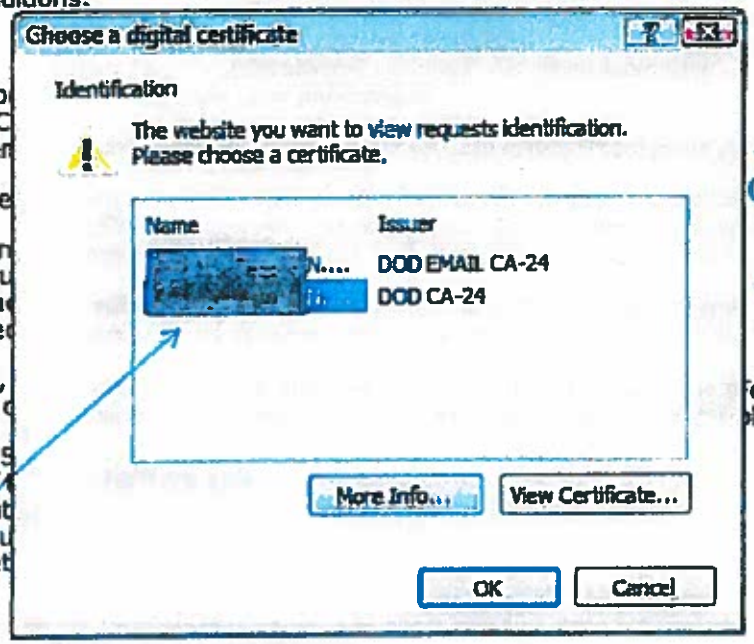
Common Access Card (CAC)

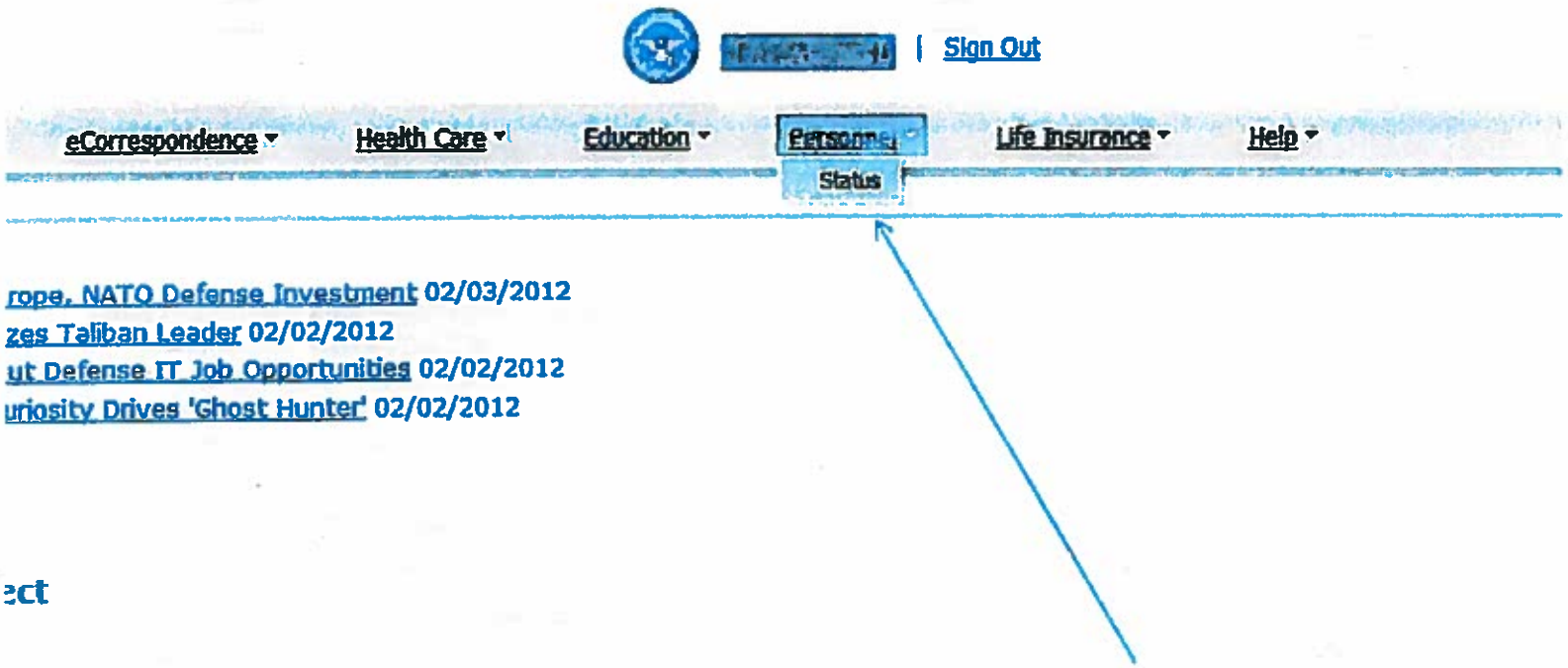
Log On

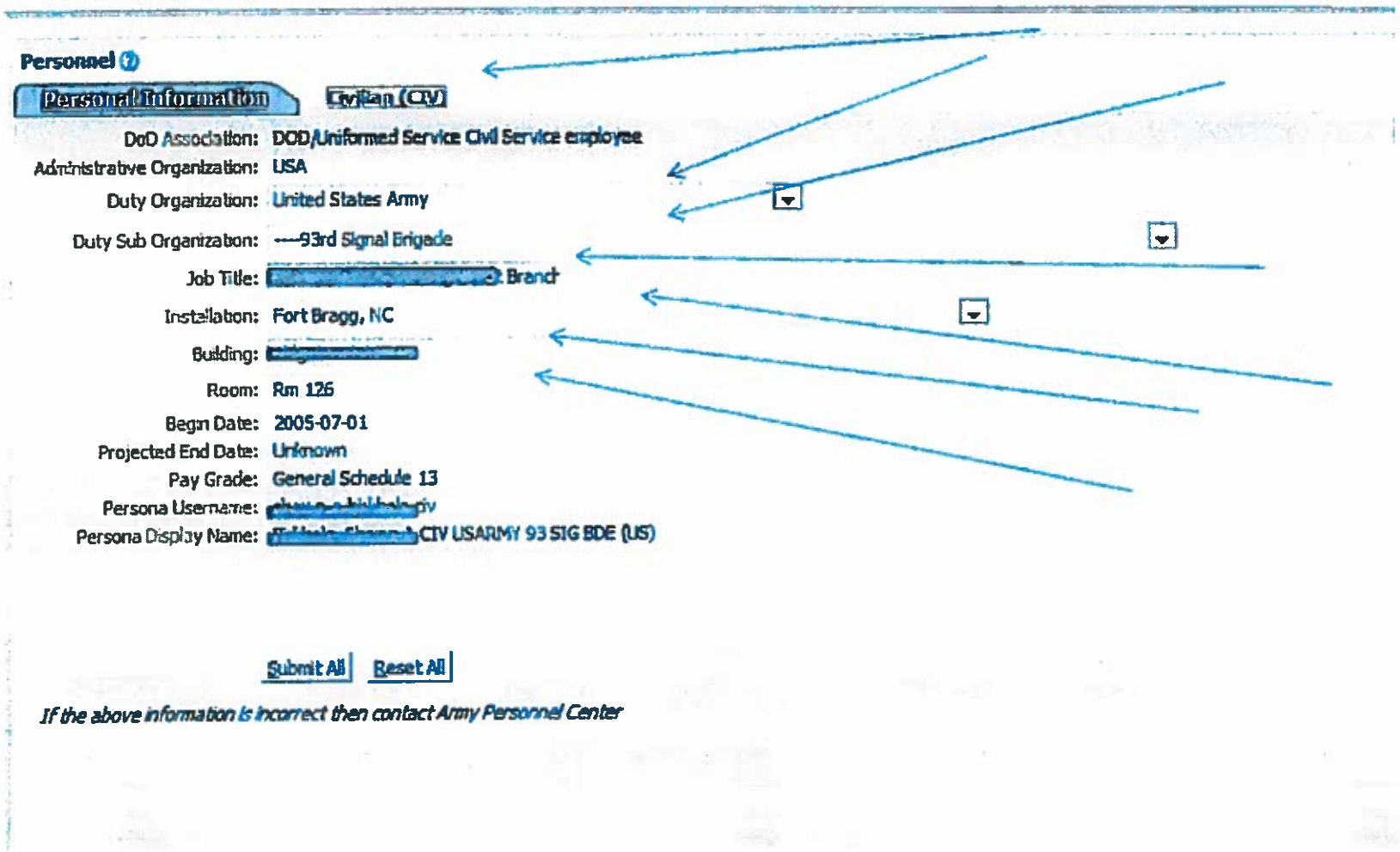
DoD Self-Service Logon (DSLogon)

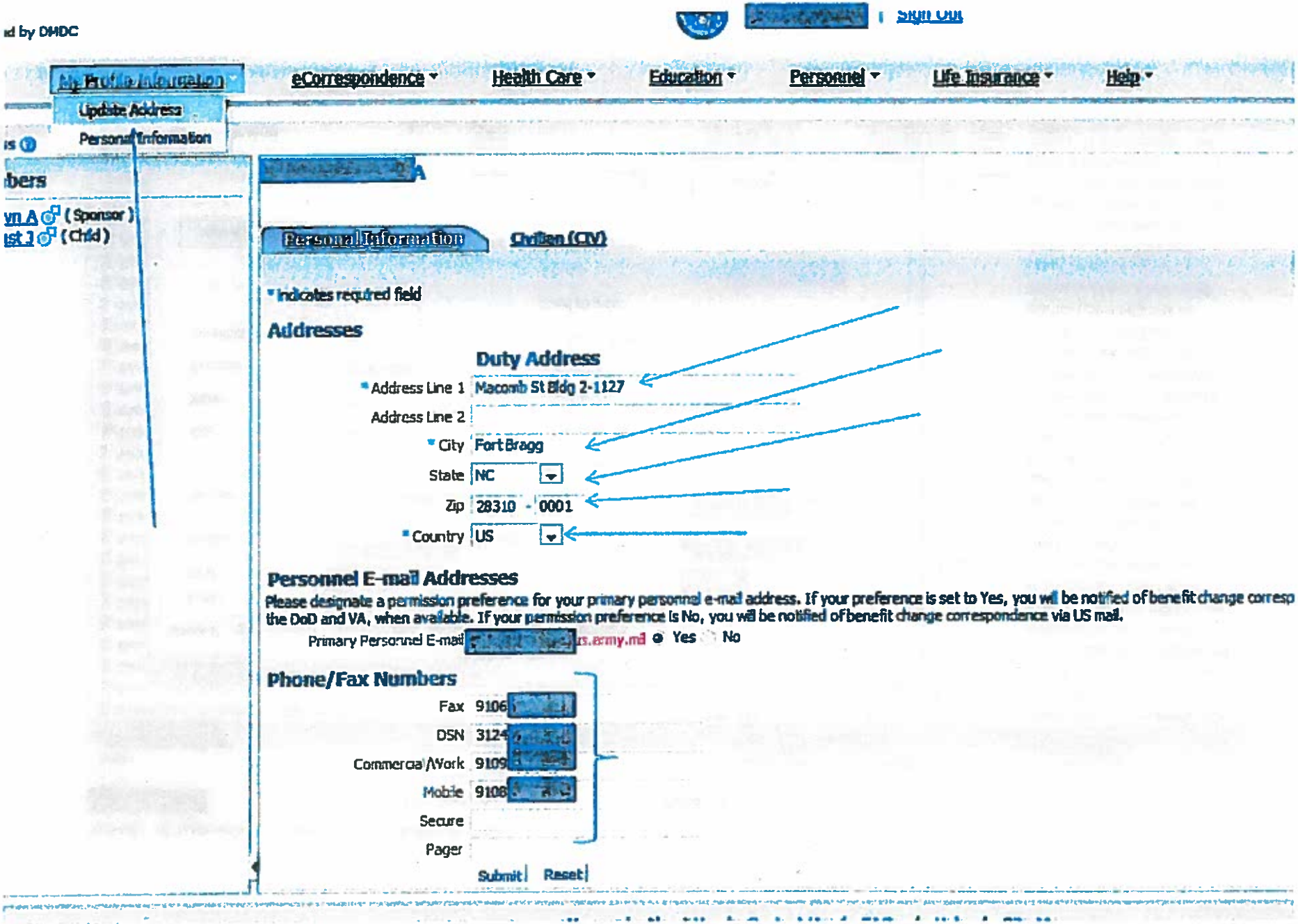
DFAS Account (myPay)

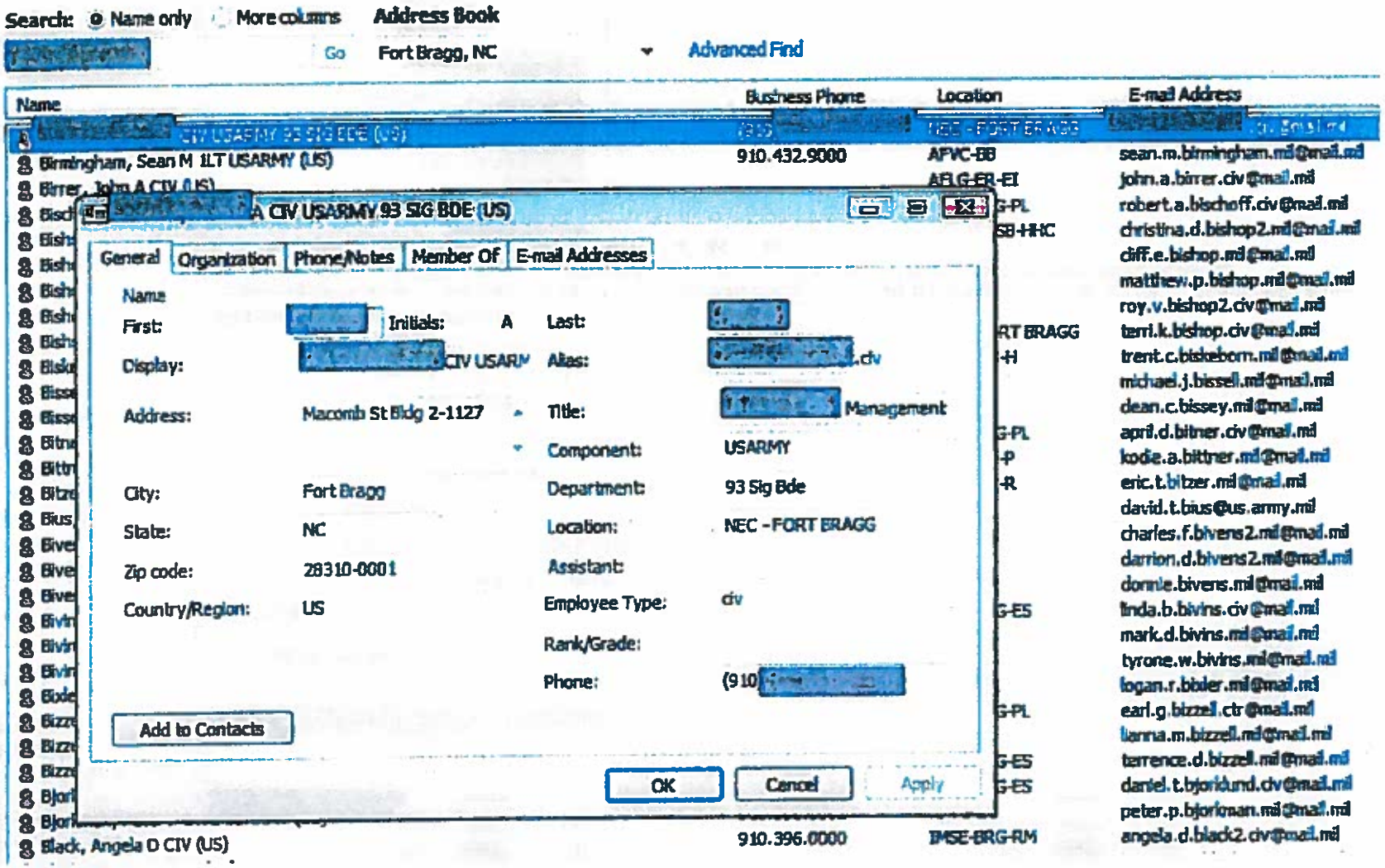
For assistance with initial login problems, please call 800-477-8227.

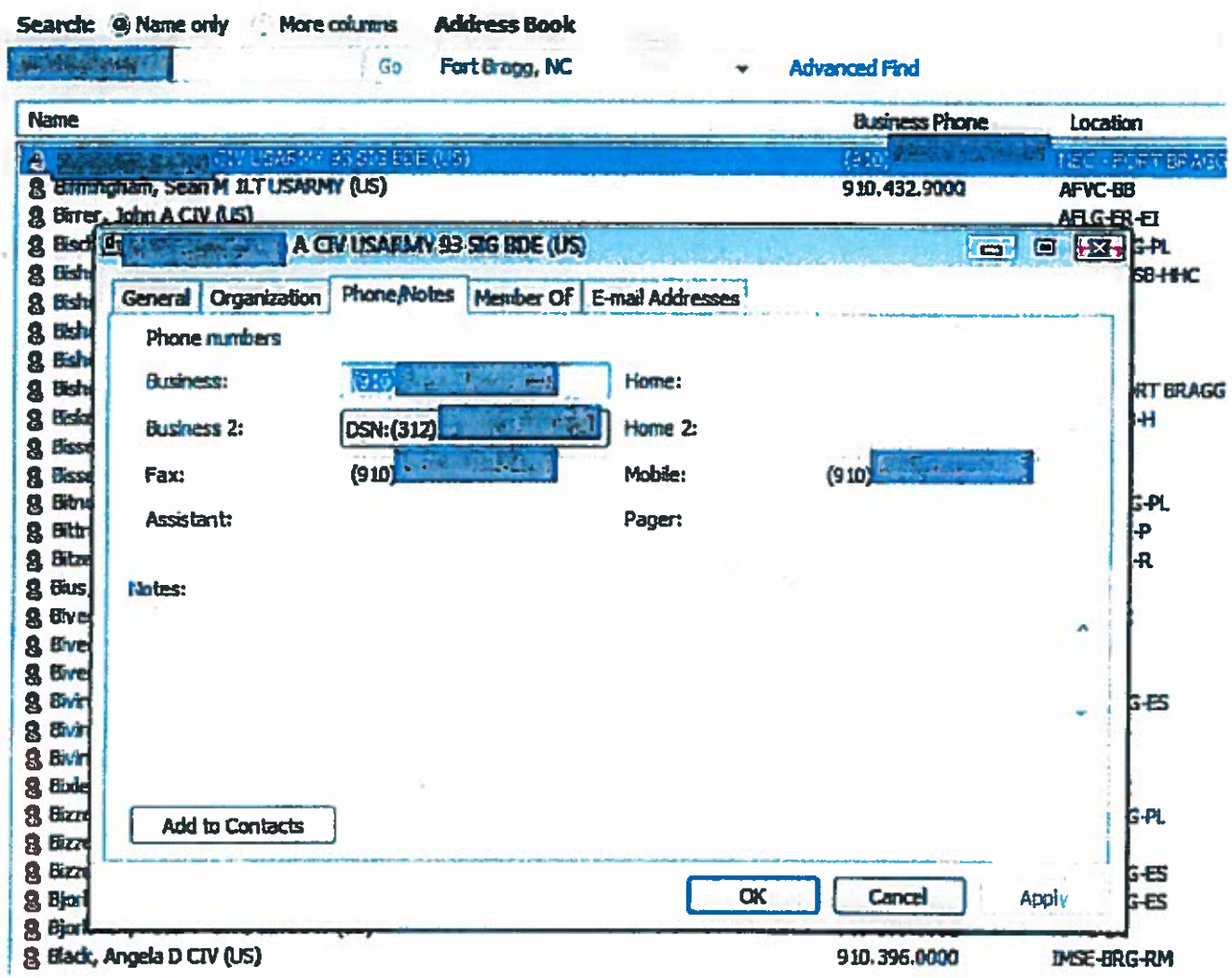



| Sign Out
eCorrespondence
Health Care
Education
Life Insurance
Help
Status
rope, NATO Defense Investment 02/03/2012
zes Taliban Leader 02/02/2012
ut Defense IT Job Opportunities 02/02/2012
uriosity Drives 'Ghost Hunter' 02/02/2012
ect


Personnel
Personal Information
Civilian (CIV)
DoD Association: DOD/Uniformed Service Civil Service employee
Administrative Organization: USA
Duty Organization: United States Army
Duty Sub Organization: ----93rd Signal Brigade
Job Title: [redacted] Branch
Installation: Fort Bragg, NC
Building: [redacted]
Room: Rm 126
Begin Date: 2005-07-01
Projected End Date: Unknown
Pay Grade: General Schedule 13
Persona Username: [redacted]
Persona Display Name: [redacted] CIV USARMY 93 SIG BDE (US)
Submit All
Reset All
If the above information is incorrect then contact Army Personnel Center


d by DHDC
Sign Out
eCorrespondence
Health Care
Education
Personnel
Life Insurance
Help
Update Address
Personal Information
Personal Information
Civilian (CIV)
* Indicates required field
Addresses
Duty Address
* Address Line 1 Macomb St Bldg 2-1127
Address Line 2
* City Fort Bragg
State NC
Zip 28310 - 0001
* Country US
Personnel E-mail Addresses
Please designate a permission preference for your primary personnel e-mail address. If your preference is set to Yes, you wil be notified of benefit change corresp
the DoD and VA, when available. If your permission preference is No, you will be notified of benefit change correspondence via US mail.
Primary Personnel E-mail
s.army.mil
Yes
No
Phone/Fax Numbers
Fax 9106
DSN 3124
Commercial/Work 9109
Mobile 9108
Secure
Pager
Submit
Reset


Search: Name only More columns Address Book
Go Fort Bragg, NC Advanced Find
Name
Business Phone
Location
E-mail Address
Birmingham, Sean M 1LT USARMY (US)
910.432.9000
AFVC-BB
sean.m.birmingham.mil@mail.mil
A CIV USARMY 93 SIG BDE (US)
General
Organization
Phone/Notes
Member Of
E-mail Addresses
Name
First:
Initials: A
Last:
Display:
Alias:
Address:
Macomb St Bldg 2-1127
Title:
Management
Component:
USARMY
City:
Fort Bragg
Department:
93 Sig Bde
State:
NC
Location:
NEC - FORT BRAGG
Zip code:
28310-0001
Assistant:
Country/Region:
US
Employee Type:
civ
Rank/Grade:
Phone:
(910
Add to Contacts
OK
Cancel
Apply
Black, Angela D CIV (US)
910.396.0000
IMSE-BRG-RM


Search: Name only More columns Address Book
Go
Fort Bragg, NC
Advanced Find
Name
Business Phone
Location
Birmingham, Sean M 1LT USARMY (US)
910.432.9000
AFVC-BB
Birrer, John A CIV (US)
A CIV USAFMV 93 SIG BDE (US)
General
Organization
Phone/Notes
Member Of
E-mail Addresses
Phone numbers
Business:
Home:
Business 2:
DSN:(312)
Home 2:
Fax:
(910)
Mobile:
(910)
Assistant:
Pager:
Notes:
Add to Contacts
OK
Cancel
Apply
Black, Angela D CIV (US)
910.396.0000
IMSE-BRG-RM

Barth, Lisa Mrs CIV USA

From: Jackiewicz, Johnny J Mr CIV USA IMCOM
Sent: Tuesday, November 30, 2010 7:15 AM
To: LEON-DL-SECURITY MANAGERS
Cc: Beasley, James CIV USA NETCOM/9TH SC A 7TH SC; Fleming, John CIV USA TRADOC; Goold, Bob Mr CIV USA TRADOC; Gundersen, Victor W Mr CIV USA TRADOC; Minton, James L Mr CIV USA TRADOC; Palmer, Victoria Mrs CIV USA TRADOC; Ramsey, Keith CIV USA TRADOC; Roberson, Phil A Mr CIV USA TRADOC; Skinner, Daniel SSG MIL USA TRADOC; Ziegler, Ron R Mr CIV USA TRADOC; Jester, Heather L Mrs CIV USA IMCOM; Tryon, Becky L Ms CIV USA IMCOM
Subject: FW: Unauthorized Disclosure of Classified Information (UNCLASSIFIED)

Importance: High

Classification: UNCLASSIFIED
Caveats: FOUO

Security Manager's / S-2's--It is imperative the following message is disseminated to the entire organization (Military, DA Civilians &
Contractors) down to the lowest level. Commanders / directors will receive this message again at the Commander / Director meeting.

Recently thousands of very sensitive and classified documents from the U.S. State Department were "leaked" and released to the public on the Wikileaks web site. This incident, along with the previous two, highlight the need to strictly enforce the importance of safeguarding national security information and related sensitive data.

All cleared government (military and civilian) and contract employees are reminded of their responsibility to protect classified and contract/OPSEC sensitive information and report known or suspected instances of unauthorized disclosures. Any downloading or copying and saving of classified data from Wikileaks to unclassified computer systems is considered spillage and will be properly investigated. Please be reminded that IT malfeasance is reportable as derogatory information and can negatively affect clearance eligibility & future systems access.

As a condition of being granted security clearance eligibility and access to classified information, a Nondisclosure Agreement (NdA) was signed attesting to the commitment to protect that information. This means there is no discussion or release of classified/unclassified sensitive information to unauthorized persons. Do not publish books or articles about classified experiences without proper protocols being executed through intelligence/security channels. Disclosure of this information, including "leaks" to the public, can compromise sensitive sources and methods, and can lead to the loss of critical capabilities, resources and even lives.
Disclosure of such information can have serious consequences not only to the military mission, but for our nation's security.

Decisive engagement by leaders at all levels is needed to ensure network users are effectively trained on the correct procedures for handling classified information and for reporting and investigating security incidents.

Again, it is all of our responsibility to protect classified and contract/OPSEC sensitive information and to be vigilant of activities that may impact national security or erode mission capability as a result of any unauthorized disclosure. Neither confirm nor deny

information contained in any articles or websites. Refer all queries for information to the Public Affairs Office (573) 563-4013, MSCoE, G-2 (Intelligence and Security), (573) 563-7278 or 902nd MI Field Office, (573) 596-0598.

Mr Steve Munsie
Command Security Manager,
G-2 (Intelligence & Security)
MSCoE & Fort Leonard Wood, MO

v/r

Mr. Johnny J. Jackiewicz
Information & Industrial Security
Office of Intelligence & Security/G-2
Comm--(573) 563-7278; DSN--676-xxxx

Classification: UNCLASSIFIED
Caveats: FOUO

Network Enterprise
Technology Command

SIPRNet Token Handling Procedures

1. Tokens are SECRET when inserted in the user's workstation and unlocked. When removed from the user's workstation, the tokens are UNCLASSIFIED and should be under the user's control.

2. The token PIN is SECRET and if written down must be stored in a container authorized for storage of SECRET information.

3. The user may be required to verify possession of the token by the Registration Authority(RA), Local Registration Authority(LRA) or Trusted Agent(TA).

4. The SIPRNet token should not be inserted into ANY NIPRNet smart card reader. If it is inadvertently inserted but the PIN is not entered, remove it immediately – it is not a security issue. If the PIN has been entered, the token should be immediately removed and the incident reported to the Information Assurance Security Officer(IASO) and RA, LRA or TA.

5. With domain aware middleware properly configured to allow only SIPRNet tokens, insertion of a NIPRNet token into SIPRNet is not a security violation unless it is apparent the NIPRNet token has become activated. Correctly configured, domain aware middleware would detect the NIPRNet token as unauthorized and block PIN entry, and block any service

NORTH ATLANTIC TREATY ORGANIZATION (NATO)
ANNUAL TRAINING FOR INDIVIDUALS WITH SIPRNET ACCESS

1. Individuals having SIPRNET access are required to receive a general **annual** NATO security briefing. This briefing explains the basic security standards and procedures for safeguarding NATO Secret, NATO Confidential, NATO Restricted, and NATO Unclassified information that you may come in contact with while utilizing the SIPRNET. This briefing does not meet NATO briefing requirements for those individuals who require continuous NATO access.

2. The four basic NATO classifications discussed herein are:

a. NATO SECRET (NS) - This security classification is applied to information the unauthorized disclosure of which would cause serious damage to NATO.

b. NATO CONFIDENTIAL (NC) - This security classification is applied to information the unauthorized disclosure of which would be damaging to the interests of NATO.

c. NATO RESTRICTED (NR) - This security classification is applied to information the unauthorized disclosure of which would be disadvantageous to the interests of NATO. The security safeguards for NATO Restricted material are similar to those of For Official Use Only information; however, NATO Restricted is considered a security classification.

d. NATO UNCLASSIFIED (NU) - This marking is applied to official information that is the property of NATO but does not meet the criteria for classification. It is similar to U.S. Government official information that must be reviewed prior to public release.

3. Safeguarding NATO Material. NATO Secret materials require continuous control and accountability. Contact the Fort Leonard Wood NATO Control Point at (573) 563-7344 or DSN 676-7344 if retention, reproduction, transmission, destruction, etc., of NS and NC materials are required. NS and NC will be safeguarded via the SIPRNET or a GSA-approved security container. Maintain administrative control of NR and NU material to preclude unauthorized access (utilize SIPRNET, GSA-approved security container, or a locked filing cabinet, book case, desk or other such container). NC, NR, and NU shall be destroyed by any means authorized for U.S. Confidential material. Segregate NATO material from U.S. classified material if stored in a GSA-approved security container.

4. Security Violations. Contact your local Security Manager, the NATO Control Point or local counterintelligence officials immediately if you find NATO material unsecured/unattended.

5. Further information is also available to users in .mil and .gov domains on the Central U.S. Registry websites:
   a. NIPRNET website is https://secureweb.hqda.pentagon.mil/cusr.
   b. SIPRNET website is http://classweb.hqda-s.army.smil.mil/cusr.

I certify that I have read and understand the above briefing declaration and agree to comply with the requirements that have been set forth.

PRINT NAME (LAST, First MI)	SIGNATURE	DATE

DEPARTMENT OF THE ARMY
U.S. ARMY ENGINEER SCHOOL AND REGIMENTAL HEADQUARTERS
14010 MSCOE LOOP, SUITE 1661
FORT LEONARD WOOD, MISSOURI 65473-8301

REPLY TO
ATTENTION OF

ATSE

1 March 2017

MEMORANDUM FOR U.S Army Registration Authority, Second Army/NETCOM, 2133 Cushing Street, Building 61801, Room 3104, Fort Huachuca, AZ 85613

SUBJECT: SIPR Token Request for Rank/Grade Full Name

1. The purpose of this memorandum is to request the issuance of SIPR tokens for the U.S. Army Engineer School Headquarters, Fort Leonard Wood, MO 65473

2. The following listed individual requires a SIPR token in order to complete daily operations at the U.S Army Engineer Regimental School. Soldier is to required t view operations orders (OPORDS), plan upcoming missions and review USR. Due to the daily requirements to ensure regulation guidelines are met, it would benefit the Army and the unit for the personnel listed below to have a SIPR token. Soldier will be the incoming Job Title of the Engineer School. The USAES, HQ S-2 has verified the need of the listed personnel.

NAME	POSITION	MOS

3. Purpose: To perform the duties as outlined in the above authority.

4. Period: Until officially released or relieved from these requirements.

5. Special Instructions: Soldier(s) will adhere to any and all DoD guidelines and regulations on maintaining accountability of SIPR tokens.

6. Point of contact for this action is sherri.l.wallace2.civ@mail.mil at 573-563-8080.

KELVIN C. NICHOLS
LTC, EN
Chief of Staff

* To be completed electronically

SYSTEM AUTHORIZATION ACCESS REQUEST (SAAR)

PRIVACY ACT STATEMENT

AUTHORITY: Executive Order 10450, 9397; and Public Law 99-474, the Computer Fraud and Abuse Act.
PRINCIPAL PURPOSE: To record names, signatures, and other identifiers for the purpose of validating the trustworthiness of individuals requesting access to Department of Defense (DoD) systems and information. NOTE: Records may be maintained in both electronic and/or paper form.
ROUTINE USES: None.
DISCLOSURE: Disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay or prevent further processing of this request.

TYPE OF REQUEST	DATE *(YYYYMMDD)*
☒ INITIAL ☐ MODIFICATION ☐ DEACTIVATE ☐ USER ID _____	

SYSTEM NAME *(Platform or Applications)*	LOCATION *(Physical Location of System)*
SIPR/NIPR	

PART I *(To be completed by Requestor)*

1. NAME *(Last, First, Middle Initial)*	2. ORGANIZATION	
3. OFFICE SYMBOL/DEPARTMENT	4. PHONE *(DSN or Commercial)*	
5. OFFICIAL E-MAIL ADDRESS first.m.last4.mil@mail.mil	6. JOB TITLE AND GRADE/RANK	
7. OFFICIAL MAILING ADDRESS	8. CITIZENSHIP ☒ US ☐ FN ☐ OTHER	9. DESIGNATION OF PERSON ☒ MILITARY ☐ CIVILIAN ☐ CONTRACTOR

10. IA TRAINING AND AWARENESS CERTIFICATION REQUIREMENTS *(Complete as required for user or functional level access.)*
☒ I have completed Annual Information Awareness Training. DATE *(YYYYMMDD)* _____

11. USER SIGNATURE	12. DATE *(YYYYMMDD)*

PART II - ENDORSEMENT OF ACCESS BY INFORMATION OWNER, USER SUPERVISOR OR GOVERNMENT SPONSOR *(If individual is a contractor - provide company name, contract number, and date of contract expiration in Block 16.)*

13. JUSTIFICATION FOR ACCESS
Require access to an email account on the (Location) SIPRNET to disseminate information over the classified network.
Enterprise Email address: first.m.last4.mil@mail.smil.mil

14. TYPE OF ACCESS REQUIRED:
☒ AUTHORIZED ☐ PRIVILEGED

15. USER REQUIRES ACCESS TO: ☒ UNCLASSIFIED ☒ CLASSIFIED *(Specify category)*
☐ OTHER _____

16. VERIFICATION OF NEED TO KNOW I certify that this user requires access as requested. ☒	16a. ACCESS EXPIRATION DATE *(Contractors must specify Company Name, Contract Number, Expiration Date. Use Block 27 if needed.)*	
17. SUPERVISOR'S NAME *(Print Name)*	18. SUPERVISOR'S SIGNATURE	19. DATE *(YYYYMMDD)*
20. SUPERVISOR'S ORGANIZATION/DEPARTMENT	20a. SUPERVISOR'S E-MAIL ADDRESS	20b. PHONE NUMBER
21. SIGNATURE OF INFORMATION OWNER/OPR	21a. PHONE NUMBER	21b. DATE *(YYYYMMDD)*

22. SIGNATURE OF IAO OR APPOINTEE	23. ORGANIZATION/DEPARTMENT	24. PHONE NUMBER	25. DATE *(YYYYMMDD)*

26. NAME *(Last, First, Middle Initial)*

27. OPTIONAL INFORMATION *(Additional information)*

AKO-S account: first.m.last@us.army.smil.mil (IF YOU HAVE ONE)

US Army TRADOC NATO Security Briefing was read and acknowledged on DDMMMYYY : NATO Briefing Acknowledgment is maintained on file locally.

the SIPRNet AUP was read and acknowledged on DDMMMYYYY : AUP is on file within ATCTS.

PART III - SECURITY MANAGER VALIDATES THE BACKGROUND INVESTIGATION OR CLEARANCE INFORMATION

28. TYPE OF INVESTIGATION		28a. DATE OF INVESTIGATION *(YYYYMMDD)*	
28b. CLEARANCE LEVEL		28c. IT LEVEL DESIGNATION ☐ LEVEL I ☐ LEVEL II ☒ LEVEL III	
29. VERIFIED BY *(Print name)*	30. SECURITY MANAGER TELEPHONE NUMBER	31. SECURITY MANAGER SIGNATURE	32. DATE *(YYYYMMDD)*

PART IV - COMPLETION BY AUTHORIZED STAFF PREPARING ACCOUNT INFORMATION

TITLE:	SYSTEM	ACCOUNT CODE
	DOMAIN	
	SERVER	
	APPLICATION	
	DIRECTORIES	
	FILES	
	DATASETS	
DATE PROCESSED *(YYYYMMDD)*	PROCESSED BY *(Print name and sign)*	DATE *(YYYYMMDD)*
DATE REVALIDATED *(YYYYMMDD)*	REVALIDATED BY *(Print name and sign)*	DATE *(YYYYMMDD)*

* To be completed electronically

SUBSCRIBER	DEPARTMENT OF DEFENSE (DOD) PUBLIC KEY INFRASTRUCTURE (PKI) CERTIFICATE OF ACCEPTANCE AND ACKNOWLEDGEMENT OF RESPONSIBILITIES

1. CERTIFICATE ACCEPTED BY

a. NAME *(Typed or printed) (Last, First, Middle Initial)*	b. UNIQUE IDENTIFICATION *(e.g., EDIPI, UID)*	
c. ORGANIZATION Network Enterprise Center (Your Org/Unit)	**d. TELEPHONE NUMBER** *(Include Area Code)*	**e. E-MAIL ADDRESS** Your SIPR Email address @mail.smil.mil

PRIVACY ACT STATEMENT

AUTHORITY: 5 U.S.C. 301, Departmental Regulation; 44 U.S.C. 3101.

PRINCIPAL PURPOSE(S): To collect personal identifiers during the certification registration process, to ensure positive identification of the subscriber who signs this form.

ROUTINE USES: Information is used in the DOD PKI certificate registration process.

DISCLOSURE: Voluntary; however, failure to provide the information may result in denial of issuance of a token containing PKI private keys.

You have been authorized to receive one or more private and public key pairs and associated certificates. A private key enables you to digitally sign documents and messages and identify yourself to gain access to systems. You may have another private key to decrypt data such as encrypted messages. People and electronic systems inside and outside the DoD will use public keys associated with your private keys to verify your digital signature, or to verify your identity when you attempt to authenticate to systems, or to encrypt data sent to you. The certificates and private keys will be issued on a token, for example a Common Access Card (CAC), another hardware token, or a floppy disk. The certificates and private keys on your token are government property and may be used for official purposes only.

Acknowledgement of Responsibilities: I acknowledge receiving my PKI private keys and will comply with the following obligations:

- I will use my certificates and private keys only for official purposes;
- I will comply with the instructions described to me today for selecting a Personal Identification Number (PIN) or other required method for controlling access to my private keys and will not disclose same to anyone, leave it where it might be observed, nor write it on the token itself;
- I understand that if I receive key management (encryption/decryption) key pairs on my token, copies of the private decryption keys have been provided to the key recovery database in case they need to be recovered; and
- I will report any compromise (e.g., loss, suspected or known unauthorized use, misplacement, etc.) of my PIN or token to my supervisor, security officer, Certification Authority (CA), Registration Authority (RA), Local Registration Authority (LRA), Trusted Agent (TA), or Verifying Official (VO), immediately.

Liability: I will have no claim against the DoD arising from use of the Subscriber's certificates, the key recovery process, or a Certification Authority's (CA's) determination to terminate or revoke a certificate. The DoD is not liable for any losses, including direct or indirect, incidental, consequential, special, or punitive damages, arising out of or relating to any certificate issued by a DoD CA.

Governing Law: DoD Public Key Certificates shall be governed by the laws of the United States of America.

f. IDENTIFICATION 1		g. IDENTIFICATION 2	
(1) TYPE *(DoD ID, Passport, etc.)* DOD ID (CAC)	(2) NUMBER	(1) TYPE *(DoD ID, Passport, etc.)*	(2) NUMBER
h. SUBSCRIBER'S SIGNATURE *(The signature provided may be a digital signature if a good fingerprint or other adequate biometric has been collected. Otherwise the subscriber must provide a handwritten signature.)*			**i. DATE SIGNED** *(YYYYMMMDD)*

2. REGISTRATION OFFICIAL PER CPS

I have personally verified the identity of the person above in accordance with the applicable CPS and have personally witnessed that person sign the form.

a. NAME *(Typed or printed) (Last, First, Middle Initial)*	b. ORGANIZATION
NEC's Info	
c. TELEPHONE NUMBER *(Include Area Code)*	**d. E-MAIL ADDRESS**
e. REGISTRATION OFFICIAL'S SIGNATURE	**f. DATE SIGNED** *(YYYYMMMDD)*

Investigation Request

CATEGORY	REQUIREMENT		INTERIM	IT LEVEL
☐ MILITARY	*IMPORTANT*: Check JPAS	☐ SECRET	☐ YES	☐ I
☐ DA CIVILIAN	before answering below!	☐ TOP SECRET	☐ NO	☐ II
☐ CONTRACTOR	☐ INITIAL	☐ SUITABILITY		☐ III
	☐ RE-INVESTIGATION	☐ PR		☐ IV
		☐ NONE		☐ NONE

SUBJECT INFORMATION

Name: (LAST) , (First) (Full Middle) --- (Military Only) MOS:

Rank: SSN: (NO Dashes) Date of Birth: (MM/DD/YYYY) / /

Country of Birth: State of Birth: City of Birth:

E-Mail Address: (Primary) E-Mail Address: (Alt)

Phone :(Primary) ☐Cell/☐Home/☐Work Phone: (Alt) ☐Cell/☐Home/☐Work

ORGANIZATION INFORMATION

Unit / Directorate: (Short Name) UIC:

SUPERVISOR INFORMATION

Name: (First) (LAST) Rank (Military Only): Title:

E-Mail Address: Phone: ☐ Cell / ☐ Work

REQUESTOR INFORMATION

Name: (First) (LAST) Title:

E-Mail Address: Phone: ☐ Cell / ☐ Work

ALTERNATE REQUESTOR INFORMATION

Name: (First) (LAST) Title:

E-Mail Address: Phone: ☐ Cell / ☐ Work

CITIZENSHIP: Verified Y ☐ N ☐

- ☐ Birth Certificate
- ☐ Certificate of Citizenship-INS
- ☐ Certificate of Naturalization
- ☐ Certification of Birth (Form DS-1350)
- ☐ Certification of Birth (Form FS-545)
- ☐ Passport
- ☐ Report of Birth Abroad (FS-240)

Doc #: _____

REMARKS:

1—***ALL* must be answered or the request will not be initiated.**
2—Applicant has 5 days to complete the application process.
3—Applicant must arrange for electronic fingerprints IMMEDIATELY.
4—All communication & coordination will be with PSIP CoE; NOT G-2.

AGENCY USE ONLY

Date Initiated. _____

TCN _____

Ticket No _____

US Army Human Resource Command Information Systems Use/Security Awareness Agreement

This agreement provides an overview of policies that apply to the use of HRC Information Systems:

1. General:

a. HRC Information Systems are available to facilitate the operational and administrative work of authorized users. These systems will be used for official government business only except for specifically authorized limited personal use IAW the Joint Ethics Regulation and will not be used for any illegitimate or fraudulent purpose. System access is not anonymous and your use constitutes consent to monitoring.

b. Users will use HRC resources responsibly and abide by normal standards of professional and personal courtesy and conduct at all times. In accessing these systems, all users agree to comply with all policies and procedures governing the use of HRC owned or supported systems. They agree to take full responsibility for all actions performed via the account assigned. Inappropriate use of these systems may be a basis for consideration of criminal or administrative disciplinary action against users. Any user who fails to comply with HRC rules and procedures will be denied system access.

c. Your Information Assurance Security Officer (IASO) is required to have you read and sign this statement and maintain it on file.

d. All users will be part of a security training and awareness program IAW Chapter 3-2, Army Regulation (AR) 25-2. The program will ensure that all users are aware of proper operational and security-related procedures and risks.

2. Environment:

a. HRC systems operate in a shared/limited resource environment processing sensitive data. As an authorized user, you have access to computer resources to do you job. Take advantage of the vast knowledge and information available through these systems to accomplish your mission, but use these resources judiciously in order to conserve our limited capabilities. Do not abuse your access.

b. HRC computer systems process defense information at the Sensitive but Unclassified (SBU) level. Information labeled SBU must be protected to ensure confidentiality, availability and integrity and may or may not require protection from foreign intelligence services or other unauthorized personnel. Examples may include information dealing with logistics, medical care, personnel management, Privacy Act data, contractual data, Freedom of Information Act information, For Official Use Only (FOUO) information and certain categories of financial data.

3.Individual guidelines:

a. Your job assignment requires your receipt of a logon ID and password that permits access to HRC information systems. Do not disclose this to anyone unless required by systems administrator, in which case you will change it afterwards. You are personally responsible for any use of your account accessed with this password.

b. Avoid any communication that could result in the disclosure of sensitive information received from HRC systems to unauthorized personnel. Information accessed will be used for official business only and disseminated only to personnel with a need to know.

c. Do not use HRC systems in a way that will interfere with your official duties, undermine readiness or reflected adversely on DOD or the Army. Your use not involve: pornography, offensive material, chain letters, unofficial advertising, personal commercial purpose or gain, soliciting, selling, game playing, illegal activities, unauthorized system access, subterfuge (using someone else's account and/or create deception as if they're responsible), inappropriately handled classified materials or other uses incompatible with public service

d. Resources will not be used in a manner that overburdens our communications systems or interferes with their performance. Do not send E-mail or make file transfers that could reasonably be expected to either cause, directly or indirectly, excessive strain on any communication facilities or unwarranted or unsolicited interference with others' use of systems.

e. Make yourself aware of and abide by the limitation and/or proper use rules for any interconnected network which you access through your account. Do not use directories other that your own, including system directories, to store files without the permission of the owner.

f. Any software on HRC systems will be legally installed and documented IAS copyright laws. Do not run any unauthorized software under your account.

g. Report any suspicious activity or erratic behavior of your system to you IASO.

4.Conscientious use of HRC systems will help avoid overburdening our scarce resources and eliminate service disruptions that could be easily avoided.

I have read the US Army Human Resource Command Information Systems Use/Security Awareness Agreement. I understand my responsibilities and I understand that my use of the system is subject to monitoring. I am accountable and responsible for my actions or actions performed by others using my account and/or privileges. If I fail to comply with the rules and procedures of this agreement, my access will be revoked and I could face criminal or administrative disciplinary action for any inappropriate use.

USER'S NAME (PRINT)	SIGNATURE	DATE

USER'S PHONE #	USER'S UNIT/SECTION/OFFICE SYMBOL

PERnet SECURITY AWARENESS BRIEFING

1. You have been assigned duties involving the use of the PERnet computer system which processes sensitive defense information at the unclassified sensitive two (US2) level. IAW Army Regulation 25-2, 14 November 2003 and is defined as follows:

US2 is unclassified information which primarily must be protected to ensure its availability, integrity and confidentiality. Such information may include logistics, medical care, personnel management, privacy act data, contractual date, and 'For Official Use Only' (FOUO) information.

2. All persons accessing an Automated Information System (AIS) will be part of a security training and awareness program IAW AR 25-2. The program will ensure that all persons responsible for managing AIS resources or who access and AIS are aware of proper operational and security-related procedures and risks. Your Information Assurance Security Officer (IASO) is required to have you read and sign this statement, and maintain it on file along with your access request.

3. Your job assignment requires receipt of logon and password that permits access to a computer system processing sensitive information. You must bear in mind that AR 25-2 requires all such password to be controlled at the highest level if sensitive information is on the system.

4. I (supervisor) am required to impress upon you the extreme need for caution and discretion in any contracts, either personal or professional. As in any interesting activity, the temptation is great to refer to your professional accomplishments. You are cautioned to avoid any conversation that could result in a disclosure of sensitive information received from PERnet systems to unauthorized personnal.

5. Personnel failing to comply with the rules and procedures of this activity will have their access revoked.

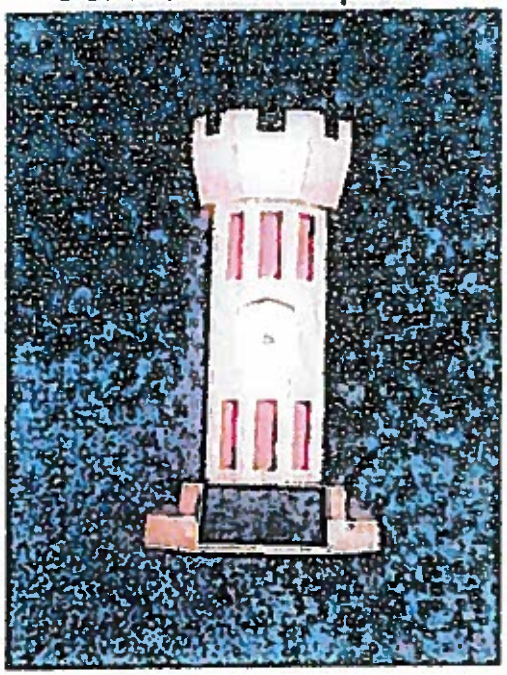
I have read the PERnet System Usage Agreement and the PERnet Security Awareness Briefing and understand my responsibilities.

USER'S SIGNATURE	DATE
SUPERVISOR'S SIGNATURE	DATE

USAES CUP AND FLOWER
Gift Options

Option 1

USAES Turret $60



12" Tall with Regimental Coin in Center

Option 2

Framed Regimental Crest $110

18" X 18" with Gold or Black Frame

Membership gets you a cup or plate for the birth of a child and a card for the death of an immediate family member.

See ~~MSG Tripp~~, EPDO, LH3623, for more Information

MSG Daniel