

RECRUIT/TRAINEE PROHIBITED ACTIVITIES ACKNOWLEDGMENT

PRIVACY ACT STATEMENT

AUTHORITY: 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; DoD Instruction 1304.33, Standardized Protection Policies Prohibiting Inappropriate Relations Between Recruiters and Recruits, and Trainers and Trainees.

PRINCIPAL PURPOSE(S): To document your understanding of the prohibitions identified in section 7 of this form.

ROUTINE USE(S): The DoD Blanket Routine Uses found at <http://dpclo.defense.gov/Privacy/SORNSIndex/BlanketRoutineUses.aspx> apply to this collection.

DISCLOSURE: Voluntary. However, if you fail to provide the requested information or complete this form, you might not be able to complete your enlistment or receive training.

INSTRUCTIONS

In accordance with DoDI 1304.33, this form will be read and signed no later than the first visit with a recruiter following a recruit's entry into the Delayed Entry Program or read and signed no later than the first day of entry-level training for a trainee. As a minimum, the signed original will be retained in the recruit's file until they enter active duty or in the trainee's file until they detach from the training command or school they are attending. Please initial beside each entry acknowledging that you have read and understand the statement.

1. RECRUIT/TRAINEE NAME (<i>Last, First, Middle</i>)	2. PAY GRADE	3. RECRUITING OFFICE/TRAINING COMMAND
4. RECRUITING OFFICE/TRAINING COMMAND ADDRESS (<i>City, State, ZIP Code</i>)	5. DATE SIGNED (YYYYMMDD)	6. SIGNATURE

7. I ACKNOWLEDGE AND UNDERSTAND THAT AS A RECRUIT OR TRAINEE, I WILL NOT:


<i>(Initial)</i> _____	a. Develop, attempt to develop, or conduct a personal, intimate, or sexual relationship with a recruiter or trainer. This includes, but is not limited to, dating, handholding, kissing, embracing, caressing, and engaging in sexual activities. Prohibited personal, intimate, or sexual relationships include those relationships conducted in person or via cards, letters, e-mails, telephone calls, instant messaging, video, photographs, social networking, or any other means of communication.
_____	b. Establish a common household with a recruiter/trainer, that is, share the same living area in an apartment, house, or other dwelling.
_____	c. Consume alcohol with a recruiter/trainer on a personal social basis.
_____	d. Attend social gatherings, clubs, bars, theaters or similar establishments on a personal social basis with a recruiter/trainer.
_____	e. Allow entry of any recruiter/trainer in my dwelling or privately-owned vehicle except to conduct official business. Exceptions are permitted for official business when the safety or welfare of the recruiter/trainer is at risk.
_____	f. Gamble with a recruiter/trainer.
_____	g. Make sexual advances toward, or seek or accept sexual advances or favors from, a recruiter/trainer.
_____	h. Lend money to, borrow money from, or otherwise become indebted to a recruiter/trainer.

8. EXCEPTIONS. Exceptions may be granted to accommodate relationships that existed prior to the start of the recruiting process or prior to the trainee starting the formal training process. These relationships include, but are not limited to, family members. Only the Recruit's or Trainee's Commander, O-4 or higher, or higher level authority, has the authority to approve these exceptions. Approved exceptions will be documented below and signed by the Recruit's or Trainee's Commander, O-4 or higher, or a higher-level authority.

DESCRIPTION OF EXCEPTION(S):

<i>(Initial)</i> _____	9. VIOLATIONS. Violations of any part of paragraph 7.a. through 7.h., not granted an exception in paragraph 8, may result in disciplinary action.
---------------------------	--

10. APPROVED BY

a. NAME (<i>Last, First, Middle Initial</i>) Jaworski, Keith A	b. TITLE Commander	c. DATE SIGNED (YYYYMMDD)	d. SIGNATURE/RANK 
---	-------------------------------------	----------------------------------	---

DOD GOVERNMENT TRAVEL CHARGE CARD (GTCC) STATEMENT OF UNDERSTANDING (SOU)

The Government Travel Charge Card (GTCC) must be used by DoD personnel to pay for all authorized expenses, to include meals, when on official travel unless an exemption is granted. This includes temporary duty travel (TDY), and per Component guidance, local and permanent change of station (PCS) travel. Refer to the Joint Travel Regulations for authorized and reimbursable travel allowances.

Cardholder must read and check off each item below.

I understand that I am being directed to:

- Confirm receipt of my GTCC and set up my PIN upon delivery.
- Ensure that my card account is open for use prior to ticketing and travel.
- Obtain tax exemption information prior to my trip from <https://www.gsa.gov/travel/plan-book/state-tax-exemption-information-for-government-charge-cards>.
- Use my card only for expenses incurred by me or when authorized for PCS travel, my eligible dependents.
- Charge my official expenses to the GTCC wherever possible rather than use cash withdrawals or another form of payment.
- File my travel voucher within five working days from returning to my PDS after completing my travel.
- Pay all my undisputed charges by the due date on my billing statement regardless of my travel reimbursement status.
- Use split disbursement to pay for all outstanding charges.
- Keep my account number, expiration date and contact information updated in DoD travel systems.
- Update my contact information with the travel card vendor when necessary.
- Notify the travel card vendor and my APC immediately if my GTCC is lost, stolen or compromised.
- Complete "Travel Card 101" training initially and refresher training every three years thereafter.
- Complete a "NEW" SOU upon arrival at each new duty assignment or every three years.

I understand that:

- Disputes must be properly submitted to GTCC issuer within 60 calendar days from the statement date or I must pay the charge.
- I am not allowed to withdraw a credit balance refund from an ATM.
- If I misuse the card, I will be subject to administrative or disciplinary action.
- Cash withdrawal fees are part of incidental expenses and not separately reimbursable.
- Online and mobile access to my account is available at CitiManager.com.

For additional information on the Travel Card, refer to your APC and the DoD GTCC Regulations (<https://www.defensetravel.dod.mil/Docs/regulations/GTCC.pdf>).

Mr. Doug Smith

434-971-3331

APC's Name:

APC's Phone Number:

20240304

Applicant or Cardholder Name/Signature

Date (YYYYMMDD)

Supervisor Name/Signature

**DISA STATEMENT OF INFORMATION SYSTEM
USE AND ACKNOWLEDGEMENT OF USER RESPONSIBILITIES**

-Basic User-

PART I

MANDATORY NOTICE & CONSENT FOR ALL DOD INFORMATION SYSTEM USER AGREEMENTS

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

- You are accessing a U.S. Government information system (IS) (which includes any device attached to this information system) that is provided for U.S. Government authorized use only.
- You will report to the proper authority within DISA any DISA or non-DISA employee that you witness or who has witnessed someone conducting malicious activity on the Network.
- If you are a supervisor, you do not have the authority to access an employee's government-issued computer and /or device. The supervisor must receive approval from General Counsel for the Agency's Counter Intelligence Representative to review the employee's government-issued computer and or device.

You consent to the following conditions:

- o The U.S. Government routinely intercepts and monitors communications on this information system for purposes including, but not limited to, penetration testing, communications security (COMSEC) monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
- o At any time, the U.S. Government may inspect and seize data stored on this information system.
- o Communications using, or data stored on, this information system are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any U.S. Government-authorized purpose.
- o This information system includes security measures (e.g., authentication and access controls) to protect U.S. Government interests--not for your personal benefit or privacy.
- o Notwithstanding the above, using an information system does not constitute consent to personnel misconduct, law enforcement, or counterintelligence investigative searching or monitoring of the content of privileged communications or data (including work product) that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Under these circumstances, such communications and work product are private and confidential, as further explained below:

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

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

- Whether any particular communication or data qualifies for the protection of a privilege, or is covered by a duty of confidentiality, is determined in accordance with established legal standards and DoD policy. Users are strongly encouraged to seek personal legal counsel on such matters prior to using an information system if the user intends to rely on the protections of a privilege or confidentiality.
- Users should take reasonable steps to identify such communications or data that the user asserts are protected by any such privilege or confidentiality. However, the user's identification or assertion of a privilege or confidentiality is not sufficient to create such protection where none exists under established legal standards and DoD policy.
- A user's failure to take reasonable steps to identify such communications or data as privileged or confidential does not waive the privilege or confidentiality if such protections otherwise exist under established legal standards and DoD policy. However, in such cases the U.S. Government is authorized to take reasonable actions to identify such communication or data as being subject to a privilege or confidentiality, and such actions do not negate any applicable privilege or confidentiality.
- These conditions preserve the confidentiality of the communication or data, and the legal protections regarding the use and disclosure of privileged information, and thus such communications and data are private and confidential. Further, the U.S. Government shall take all reasonable measures to protect the content of captured/ seized privileged communications and data to ensure they are appropriately protected.
 - o In cases when the user has consented to content searching or monitoring of communications or data for personnel misconduct, law enforcement, or counterintelligence investigative searching, (i.e., for all communications and data other than privileged communications or data that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants), the U.S. Government may, solely at its discretion and in accordance with DoD policy, elect to apply a privilege or other restriction on the U.S. Government's otherwise-authorized use or disclosure of such information.

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

PART II

DISA STATEMENT OF INFORMATION SYSTEM USE AND ACKNOWLEDGEMENT OF USER RESPONSIBILITIES FOR UNCLASSIFIED AND CLASSIFIED

FOR AUTHORIZED ACCESS:

I will use DISA Information Systems for official use and authorized purposes only in accordance with DoD 5500.7-R, Joint Ethics Regulation. I will not introduce or process data which the Information System has not been specifically authorized to handle. I understand that all information processed on DISA- controlled Information Systems is subject to monitoring. This includes email and web browsing. I may also be held both criminally and financially responsible for any damages that may occur to the network, systems, other electrical and non-electrical equipment, or computing devices, if my actions are determined to be deliberate, willful, or malicious.

I understand the need to protect all passwords at the highest level of data they secure. I will not share my password(s) or accounts(s) information with coworkers or other personnel not authorized to access the information system.

I understand that I am responsible for all actions taken under my account(s) either as an authorized or privileged user. I will not attempt to "hack" the network, any connected Information Systems, or gain access to data which I am not authorized to access.

I understand my responsibility to appropriately protect and label all output generated under my account (to include printed materials, USB devices, floppy disks, and downloaded hard disk files).

I understand, I must have requisite security clearance and documented authorization (approved by my supervisor) of my need-to-know before accessing DISA/DoD information and information systems.

I understand my responsibility to ensure Privacy Act, and other protected personal information (such as personally identifiable information is protected while it is being processed or accessed. In computer environments outside the DISA physical data processing installations requiring access to DISA information and information systems (such as remote job entry stations, terminal stations, minicomputers, microprocessors, and similar activities), I know I must ensure appropriate protection of personal and sensitive data.

Information system:

I am accessing a U.S. Government information system (as defined in CNS SI 4009) that is provided for U.S. Government-authorized use only. I understand I must complete designated IA training before receiving system access.

I understand that security protections may be utilized on DISA information systems to protect certain interests that are important to the Government. For example, passwords, access cards, encryption, or biometric access controls provide security for the benefit of the Government. These protections are not provided for my benefit or privacy and maybe modified or eliminated at the Government's discretion.

I understand that I am prohibited from the following:

- Introducing classified information into an unclassified system or environment.
- Accessing, storing, processing, displaying, distributing, transmitting, or viewing material that is abusive, harassing, defamatory, vulgar, pornographic, profane, racist, promotes hate crimes, or subversive in nature, or objectionable by nature to include; material that encourages criminal activity or violates any applicable local, state, Federal, national, or international law.
- Violating the established security, release, and protection policies for information identified as Classified, Proprietary, Controlled Unclassified Information (CUI), For Official Use Only (FOUO), or Privacy Act- protected during the information handling states of storage, process, distribution or transmittal of such information.
- Obtaining, installing, copying, pasting, transferring, or using software or other materials obtained in violation of the appropriate vendor's patent, copyright, trade secret, or license agreement. This includes peer-to-peer file sharing software or games.
- Installing any unauthorized software (e.g., games, entertainment software) or hardware (e.g., sniffers).
- Knowingly writing, coding, compiling, storing, and transmitting. Or transferring malicious software code, to include viruses, logic bombs, worms, and macroviruses.
- Engaging in prohibited political activity.
- Using the system for personal financial gain such as advertising or solicitation of services or sale of personal property (e.g., eBay), or stock trading (i.e., issuing buy, hold and/or sell directions to an online broker).
- Engaging in fundraising activities, either for profit or non-profit unless the activity is specifically approved by the Command (e.g., Command social event fundraisers, charitable fund raisers, etc.).
- Gambling, wagering, or placing of any bets.

- Writing, forwarding, or participating in chain letters.
- Posting personal web pages, using my personally-owned information technology (IT such as personal electronic devices (PEDs), personal data assistants (PDAs), laptops, thumb drives etc.), or non-DISA-controlled information technology on DISA-controlled computing assets.
- Any other actions prohibited by DoD 5500.7-R or any other DoD issuances.
- Personal encryption of electronic communications is strictly prohibited and can result in the immediate termination of access.

I will immediately report any person suspected of engaging in, or any other indication of, computer network intrusion unexplained degradation or interruption of network services, or the actual or possible compromise of data or file access controls to the appropriate Information Assurance (IA) Management or senior IA Technical Level representatives. I will not install, modify, or remove any hardware or software (i.e. freeware, shareware, security tools. etc.) without written permission and approval from the Information Assurance Manager (IAM) or senior IA Technical Level representative. I will not remove or destroy system audit, security, event, or any other logs without prior approval from the IAM or senior IA Technical Level representative.

I will not introduce any unauthorized code, Trojan horse programs, malicious code, or viruses into DISA information systems or networks.

I will not allow any user access to the network or any other connected system that is not cleared without prior approval or specific guidance of the IA Management.

I will not use any DISA controlled information systems to violate software copyright by making illegal copies of software.

I agree to notify the organization that issued the account when access is no longer required.

ALL MUST READ:

I understand that failure to comply with the requirements of this User Agreement will be reported and investigated. The results of investigation may result in one or all of the following actions:

- Immediate revocation of system access and/or user privileges
- Job counseling, admonishment
- Revocation of Security Clearance
- Uniform Code of Military Justice and/or criminal prosecution
- Disciplinary action, reassignment, discharge, or loss of employment

I HAVE READ, UNDERSTAND, AND WILL COMPLY WITH THE REQUIREMENTS SET FORTH IN THIS AGREEMENT. IN THE EVENT OF CONFLICT, PART I TAKES PRECEDENCE OVER PART II ABOVE.

I have read the attached Non-Compliance Activity Disciplinary Actions document.

First Name:

Last Name:

Organization:

Enterprise Email:
(e.g., civ@mail.mil, ctr@mail.mil, mil@army.mil)

Date:
(DD-MMM-YYYY)

Signature:

If you have trouble submitting this form via the Submit button, send to:
disa.pentagon.jsp.mbx.submissions@mail.mil