Commander of Naval Air Training

Student Check-In Process

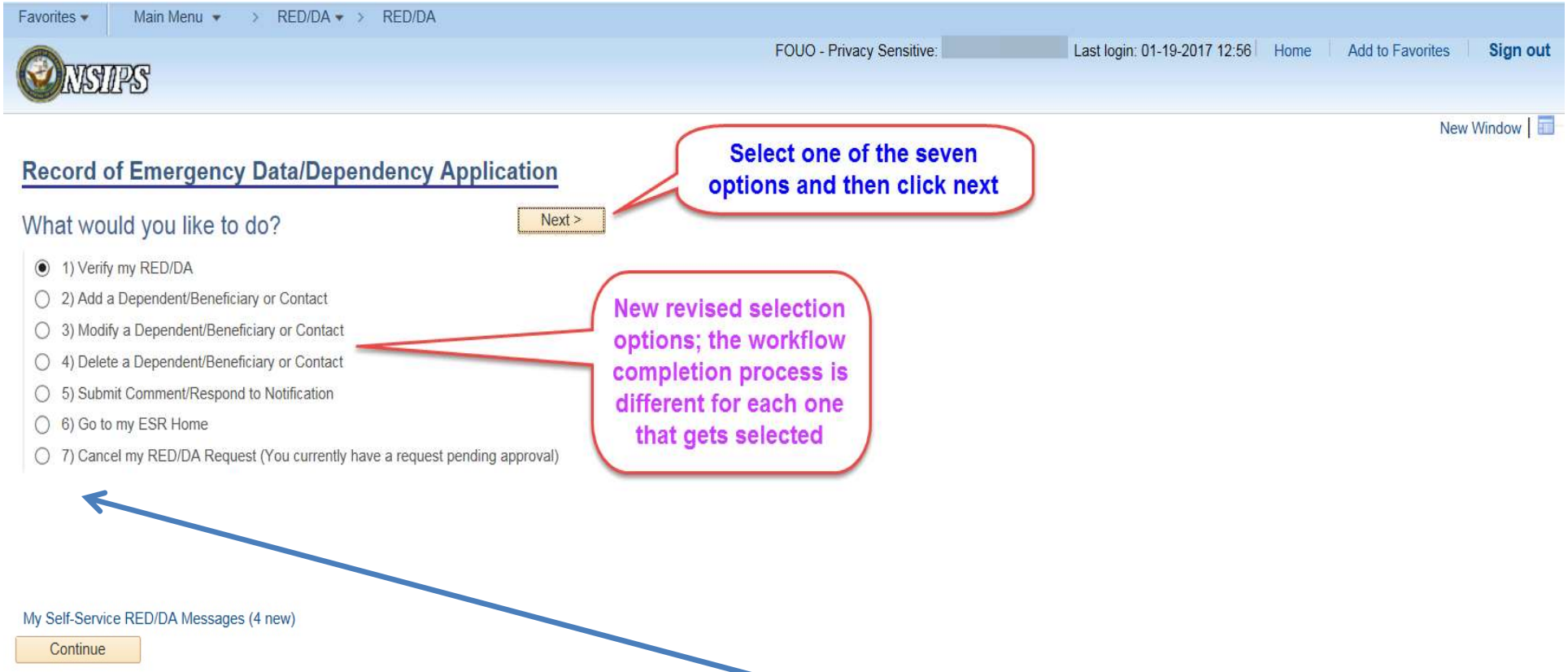
RED DA Self-Service Training

New Self-Service Workflow

Changes to NSIPS RED DA

DD 93 & NAVPERS 1070/602

RED DA Member Self-Service Menu Options

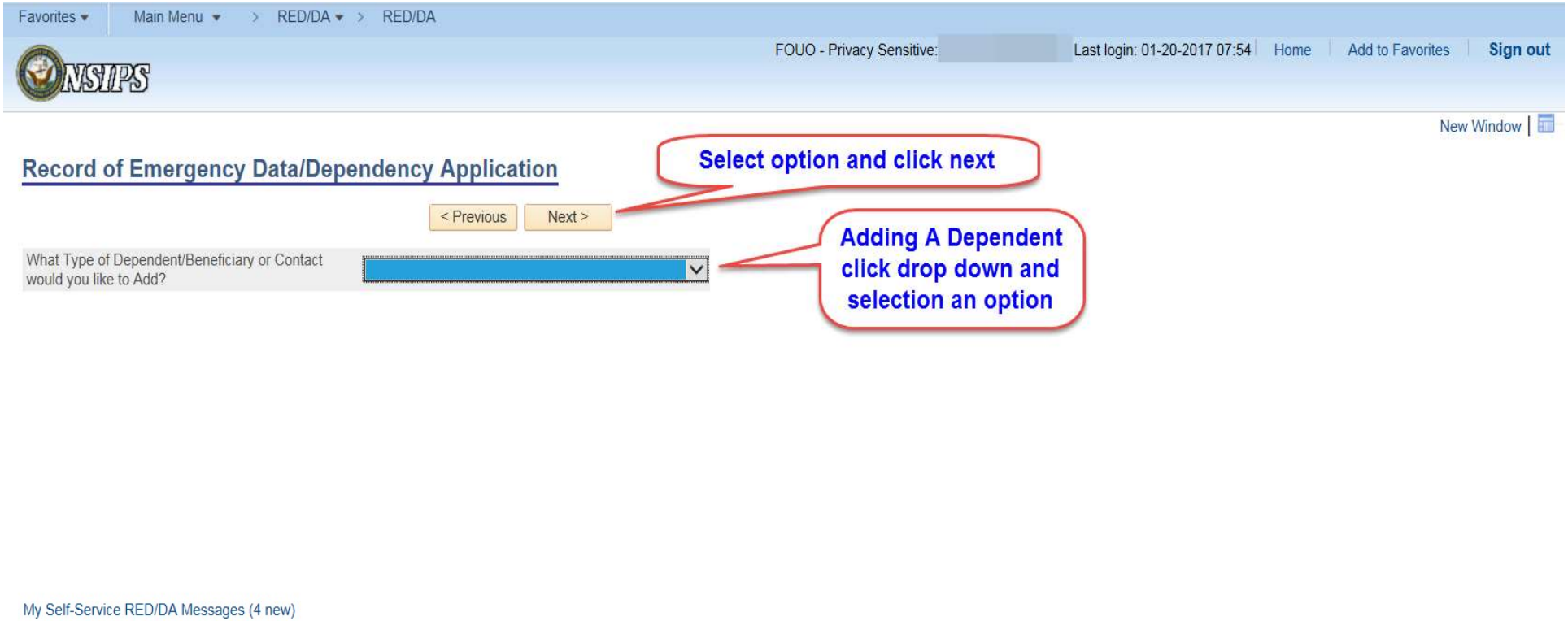


Select one of the seven options and then click next

New revised selection options; the workflow completion process is different for each one that gets selected

If #7 exist then the Service Member should click "Continue"; as a RED DA transaction is still pending in the application. This will take you to the pending application for you to complete.

Add Dependents Options



Add Dependent Information

Favorites ▾ | Main Menu ▾ > RED/DA ▾ > RED/DA

NSIPS

FOUO - Privacy Sensitive: Last login: 01-20-2017 07:54 | Home | Add to Favorites | Sign out

New Window

Step 1 of 4

1 2 3 4

Next >

RED/DA Dependent/Beneficiary/Other Contact

Information related to the dependent/beneficiary/contact.

*Name: TEST,MARY T

*Relationship: Daughter

*Birthdate: 01/20/2017

*Dependent: Dependent

Certification Date:

Recertification Date:

Enter full name as shown on birth certificate (Last Name, First Name and Middle Name)

Select Dependent or Not Dependent

Select Relationship and Enter Date of Birth

Is this Person...

A full time student over the age of 21? No

Physically or mentally incapacitated? No

Living with a custodian or legal guardian? No

Child or Dependent Support

Are there child or dependent support payments? No

Designations

Authorized Bedside Travel No

Authorized Funeral Travel No

PADD No

(Person Authorized to Direct Disposition of Remains)

Relationship:

☐ Other Person to Notify

☐ Notify if Missing

☐ Do Not Notify Due To Ill Health

Unpaid Pay / Allowances	Allotment if Missing	Gratuity Pay

Identify Address & Phone Contact

Favorites ▾ | Main Menu ▾ > RED/DA ▾ > RED/DA

NSIPS

FOUO - Privacy Sensitive: Last login: 01-20-2017 07:54 | Home | Add to Favorites | Sign out

New Window

Step 2 of 4

1 2 3 4

< Previous | Next >

Address Details

Address information for TEST,MARY T.

Select one of the address options or enter address below

- [ ] Resides with Service Member?
- [ ] Resides with Service Member's Spouse?
- [ ] Resides with Service Member's Mother?
- [ ] Resides with Service Member's Father?
- [ ] Command Sponsored?
- [ ] Same phone number as Service Member?

Select phone number option or enter phone number below

Dependent/Beneficiary/Other Contact Address

Address

*Address 1:

Address 2:

Address 3:

*City: County:

*State: *Postal:

*Country: US United States

Phone Numbers

Primary Phone

*Phone Type: *Telephone: Domestic Indicator:

Alternate Phone

Phone Type: Telephone: Domestic Indicator:

Email Address

Upload PDF Supporting Documents

Upload supporting documentation (birth certificate, marriage license, divorce decree, etc) Note: PDF documents only

Ensure you view your attachment

Mass Update Emergency Data

Favorites ▾ | Main Menu ▾ > RED/DA ▾ > RED/DA

NSIPS

FOUO - Privacy Sensitive: [redacted] Last login: 01-24-2017 13:13 | Home | Add to Favorites | **Sign out**

New Window

RED/DA Summary

Emplid: [redacted] **Current UIC:** [redacted] **Service:** *Navy*

New Dependent/Beneficiary/Other Contact

Add

If more family member need to get added click here and select a drop down option

Certification/Recertification Dates

As you can see I add my spouse and 3 children

				Relationship	Unpaid Pay / Allowances	Allotment if Missing	Gratuity Pay	PADD	Auth Bedside Travel	Auth Funeral Travel	Other Person to Notify	Notify if Missing	Do Not Notify Due to Ill Health	Delete
01	TEST,SPOUSE		Dependent	Spouse	80%	Max(100%)	Max(100%)	Yes	Yes	Yes	☐	☑	☐	Delete
02	[redacted]	Living	Dependent	Father	20%	00%	00%	No	No	No	☐	☐	☐	Delete
03	[redacted]	Living	Not Dependent	Mother	00%	00%	00%	No	Yes	No	☐	☐	☐	Delete
04	[redacted]		Not Dependent	Brother	00%	00%	00%	No	No	Yes	☐	☑	☐	Delete
05	TEST,TEST		Dependent	Daughter	00%	00%	00%	No	Yes	Yes	☐	☑	☐	Delete
06	ADD,A KID		Dependent	Daughter	00%	00%	00%	No	No	No	☐	☐	☐	Delete
07	TEST,DAUGHTER		Dependent	Daughter	00%	00%	00%	No	No	No	☐	☐	☐	Delete
08	[redacted]		Dependent	Son	00%	00%	00%	No	No	No	☐	☐	☐	Delete
	Summary				100%	100%	100%							

Click Comments to send message to PSD with package

Comments

Now select all your Record of Emergency Data information; only one PADD; upto 3 can be selected for Bedside and Funeral Travel.

Save for Later | Back | Continue

Status: Request Awaiting Approval

Click Continue if all information is captured or Save for Later

Member Self-Service Continues

Favorites | Main Menu > RED/DA > RED/DA

NSIPS

FOUO - Privacy Sensitive: Last login: 01-24-2017 13:13 | Home | Add to Favorites | Sign out

Emplid: **Current UIC:** **Service:** *Navy*

Effective Date: 05/24/2013

Member's Marital Status

*Currently: Married *On: 04/01/2016

Place of Marriage ...

*City:

*State: *Country: US

Modify/Add Spouse

Member's Previous Marriage

*Previously Married? No

Dissolved...

On: By:

City:

State: Country: US

***Religion**

EA Anglican Catholic Church

***Official Email Address**

Edit Official Email

***Phone** Find | First 1 of 1 Last

Phone Type	Telephone	Domestic Indicator
Cellular		Domestic Phone

Other Email Addresses Find | First 1-2 of 2 Last

Email Type	Email Address
Business	noreply@navy.mil
Home	noreply@navy.mil

***Current Address** Find | First 1 of 1 Last

Address Type	Effective Date	Foreign Address Type	Country	Address
HOME	10/10/2013	Domestic	United States	

Edit My Phone, Other Email Addresses, Current Address

Save for Later | Back | Continue

Status: Request Awaiting Approval

Update any information that is not correct

Update Religion preference

Update your Official Email Address

Verify your phone contact information

Verify your Current Home Address

If Home Address, Phone or other Email Addresses is not correct then click Edit to update this information. These changes will update dependents who share your home address and phone number

Click Continue when Finished

Verify or Add Supporting Documents

Favorites | Main Menu > RED/DA > RED/DA

FOUO - Privacy Sensitive: Last login: 01-24-2017 13:13 | Home | Add to Favorites | Sign out

NSIPS

Attachments and Remarks

Emplid: **Current UIC:**

Upload Supporting Documentation (Birth Certificate, Marriage License, Divorce Decree, etc)

Supporting Documentation

Upload Supporting Documentation

Add

The following action requires supporting documentation:

You are attempting to add your father as a dependent. You must upload the DFAS dependency determination approval letter when prompted.

Attach To	File Name	Attachment Type	Description	View Attachment	Validated	Delete
07 - TEST,DAUGHTER	Birth_Cert.pdf	Birth Certificate		View Attachment		Delete
05 - TEST,TEST	Birth_Cert.pdf	Birth Certificate		View Attachment		Delete

Verify your attachments are correct and legible

Remarks: DD Form 93 (Service Member Only)

Form Block 14

Remarks: NAVPERS 1070/602 (Service Member Only)

Form Block 46

Remarks: NAVPERS 1070/602 (Clerk/Supervisor Only)

Form Block 49

Find | View All First 1 of 1 Last

Clause 1 Sequence Number: 1

Description:

RECEIPTS NEW CHECK IN

NAVPERS 1070/602 UPDATED DUE TO NEW CHECK IN:
DTROB:
BAH TYPE:
//UPDATED BY: MM/DD/YYYY.

Click Continue when Finished or Save for Later if you don't have all supporting documents to upload

Save for Later | Back | Continue

Status: Request Awaiting Approval

Wills, Life Insurance or Other Valuable Papers

Favorites ▾ | Main Menu ▾ > RED/DA ▾ > RED/DA

NSIPS

FOUO - Privacy Sensitive: | Last login: 01-25-2017 08:00 | Home | Add to Favorites | Sign out

New Window |

Will & Life Insurance

Emplid: **Current UIC:** **Service:** *Navy*

Vital Documents

Summary | Address | Additional Remarks

Document Type	Description	View/Edit	Delete
Will	ABC WILL	View/Edit	Delete

*Document Type Life Insurance | Add Vital Document Data

Save for Later | Back | Continue | Status: Request Awaiti Approval

Life Insurance Policy information added with comments for Family

Complete by selecting from drop down either Will, Insurance or Other Valuable Papers

Click Continue after information has been added or if you have no information to add

Click Ok when Finished

Life Insurance

*Company: ABC LIFE INSURANCE Seq#: 1

*Policy Number: 99999999

*Address1: 123 BOX RD

Address2:

*City: MILLINGTON

*State: TN County: SHELBY

*Country: US *Postal Code: 38054

Additonal Remarks: This Insurance is for additional coverage while deployed in a combat zone.

OK | Cancel

Verification

Favorites ▾ | Main Menu ▾ > RED/DA ▾ > RED/DA

NSIPS

FOUO - Privacy Sensitive: Last login: 01-25-2017 08:00 | Home | Add to Favorites | **Sign out**

New Window |

Verification

Emplid: **Current UIC:** **Service:** *Navy*

Status: Request Awaiting Approval

Verify your original to new information added

Summary of Changes for Spouse 01: TEST,SPOUSE

Item	Original Information	New Information
Spouse Details		
Allotment if Missing	Max(100%)	80%

Summary of Changes for Father 02:

Item	Original Information	New Information
Parent Details		
Dependent	Not Dependent	Dependent
Birthdate	(n/a)	1942-01-01
Certification Date	(n/a)	2016-01-01
Recertification Date	(n/a)	2017-01-01
Authorized Funeral Travel	Y	N
Address		
Resides With Custodian/Legal Guardian?	(n/a)	Yes
Same Phone Number As Service Member?	Yes	No
Address 1		
City		
State		
Zip Code		

Ensure date of birth is correct. Is this a dependent or not dependent? Ensure you upload supporting documentation for dependent adds

Ensure address information is correct

No Changes for Mother 03:

Item	Original Information	New Information

Verification Continues

Favorites ▾ | Main Menu ▾ > RED/DA ▾ > RED/DA

NSIPS

FOUO - Privacy Sensitive: Last login: 01-25-2017 08:00 | Home | Add to Favorites | Sign out

Summary of Changes for

Item	Original Information	New Information
Dependent/Beneficiary/Contact Details		
Name	(n/a)	
Relationship	(n/a)	Son
Birthdate	(n/a)	2017-01-16
Dependent	(n/a)	Dependent
Authorized Bedside Travel	(n/a)	N
Authorized Funeral Travel	(n/a)	N
PADD	(n/a)	N
Unpaid Pay / Allowances	(n/a)	00%
Allotment if Missing	(n/a)	00%
Gratuity pay	(n/a)	00%
Student		
A Full Time Student Over The Age Of 21?	(n/a)	No
Incapacitated		
Physically Or Mentally Incapacitated?	(n/a)	N
Address		
Resides With Service Member?	(n/a)	Yes
Resides With Service Member's Spouse?	(n/a)	No
Resides With Service Member's Mother?	(n/a)	No
Resides With Service Member's Father?	(n/a)	No
Command Sponsored?	(n/a)	No
Same Phone Number As Service Member?	(n/a)	Yes
Address 1	(n/a)	
City	(n/a)	
State	(n/a)	
Zip Code	(n/a)	
Country	(n/a)	US
Phone		

Verify information on birth of Son; does it reflect the correct information on the birth certificate. Ensure supporting documentation is uploaded as a PDF document

If you child is a Full-Time Student age 21-23 this must reflect a Yes and supporting document from the College is required to be annually updated and reported

Don't forget that separate reporting is required to DEERS within 30 days of dependency status changes via the RAPID Office (ID Card Lab). They require the same reporting documentation to enroll or terminate your dependent(s) in DEERS

Verification Continues

Favorites ▾ | Main Menu ▾ > RED/DA ▾ > RED/DA

NSIPS

FOUO - Privacy Sensitive: Last login: 01-25-2017 08:00 | Home | Add to Favorites | Sign out

Domestic Indicator	(n/a)	Domestic Phone

Personal Data Change Summary

Item	Original Information	New Information
Religion		
Religion Code	NO	EA
Official Email Address		
Emailid	noreply@navy.mil	

Ensure Religion preference and Official Email Address are correct

Supporting Documentation

Attached To:	File Name	Attachment Type	Description	Validated	View Attachment
07 - TEST,DAUGHTER	Birth_Cert.pdf	Birth Cert		☐	View Attachment
05 - TEST,TEST	Birth_Cert.pdf	Birth Cert		☐	View Attachment

Ensure all supporting documentation is uploaded as PDF and View each attachment to be correct and legible

Remarks: DD Form 93 (Service Member Only)

Form Block 14

Remarks: NAVPERS 1070/602 (Service Member Only)

Form Block 46

Remarks: NAVPERS 1070/602 (Clerk/Supervisor Only)

Clause	Description	Text
1	RECEIPTS NEW CHECK IN	NAVPERS 1070/602 UPDATED DUE TO NEW CHECK IN: DTROB: BAH TYPE: //UPDATED BY: MM/DD/YYYY. IT IS MY RESPONSIBLITY TO NOTIFY MY PERSONNEL OFFICE/SHIP'S OFFICE OR CSD/PSD OF ANY CHANGES TO MY

Verification Final Actions

Favorites Main Menu > RED/DA > RED/DA

NSIPS
NAVY STANDARD INTEGRATED PERSONNEL SYSTEM

FOUO - Privacy Sensitive: Last login: 06-02-2017 07:19 Home Add to Favorites Sign out

Phone	(n/a)	555-555-5555

Supporting Documentation

Attached To:	File Name	Attachment Type	Description	Validated	View Attachment
				☐	View Attachment

Remarks: DD Form 93 (Service Member Only)

Form Block 14

Resubmit

Remarks: NAVPERS 1070/602 (Service Member Only)

Form Block 46

Resubmit

Remarks: NAVPERS 1070/602 (Clerk/Supervisor Only)

Clause	Description	Text

Comments

Forms

NAVPERS 1070/602 ★Signature Required

DD Form 93 ★Signature Required

Upload Signed Forms

Save for Later | Back | Submit | Status: Not Submitted

Service Member can make an open comment but in the Attachment & Remark Section. Hit the Back key below if you wish to add comments. 'Resubmit' in these comment blocks (14 & 46) can be used if you get a feedback email or CPPA response your transaction has failed to be accepted in the OMPF. Most failures occur because Compatibility View and/or your Adobe application does not have the proper settings established by the User. Please ensure you contact your CPPA or NSIPS Helpdesk for Steps 1-3 preceding supporting documentation need for RED DA

Now digitally sign your documents if you see "Signature Required" below each form. When you digitally sign; ensure you select the non-email certificate when electronically signing.

Click Submit when finished or click Back if any of the above information needs to be corrected. Click Save for Later if more time is need to complete.

Self-Service DD 93Forms Process

- On Verification Page, open RED document (DD 93)
- Ensure you see the following image on top of the DD 93; if you don't see the black ribbon then it mean your CAC certs could not be validated. You will have to complete Steps 1-3 in the supporting documents that deals with the setting of Internet Explorer or Mozilla Firefox and Adobe. Once the application setting are completed above; go back to NSIPS verification page and see if the Adobe document now displays the Black Ribbon as seen in Illustration below.

- If you have to perform step 1-3 above because the Black Ribbon is not displayed then close the RED document within the application (Click small grey x on open URL tab page for form to close correctly) "Do NOT click submit in form"

DD 93 Digital Signature

- If all information is correct digitally sign your document

DD FORM 93, JAN 2008 PREVIOUS EDITION IS OBSOLETE. Submit PAGE of

Step 2: Click Submit after verification of signature automatically occurs

1. NAME *(Last, First, Middle Initial)*		2. SSN
15. SIGNATURE OF SERVICE MEMBER/CIVILIAN *(Include rank, rate, or grade if applicable)*	16. SIGNATURE OF WITNESS *(Include rank, rate, or grade as appropriate)*	17. DATE SIGNED *(YYYYMMDD)*
	Not Required	

Step 1: Digitally sign here with your non-email certificate

- Do NOT Print this form when open; only print the form if needed from RED DA Inquire. This document will pull from your OMPF which make it official and can be printed. If document is not in your OMPF then the transaction may have failed; your will get an email notification from NSIPS if the transaction failed to be applied to your OMPF.

Self-Service NAVPERS 1070/602

- On Verification Page, open DA document (NAVPERS 1070/602) which is also know as the Page 2.
- Ensure you see the following image on top of the NAVPERS 1070/602; if you don't see the black ribbon then it mean your CAC certs could not be validated. You will have to complete Steps 1-3 in the supporting documents that deals with the setting of Internet Explorer or Mozilla Firefox and Adobe. Once the application setting are completed above; go back to NSIPS verification page and see if the Adobe document now displays the Black Ribbon as seen in Illustration below.

- If you have to perform step 1-3 above because the Black Ribbon is not displayed then close the RED document within the application (Click small grey x on open URL tab page for form to close correctly) "Do NOT click submit in form"

NAVPERS 1070/602 Digital Signature

- If all information is correct digitally sign your document

47. MEMBER SIGNATURE:	Unofficial Member Copy	48. DATE (Y

Digitally sign here with your non-email certificate

- Click Submit on form after verification of digital signature automatically occurs in form

50. APPROVED: ☐YES ☐NO	51. VERIFYING OFFICIAL SIGNATURE:	52. DATE (*YYYYMMDD*):
53. VERIFYING OFFICAL NAME (*printed or typed*):	54. TITLE: Personnel Supervisor, By Dir C.O.	

Click Submit

Submit

- Do NOT Print this form when open; only print the form if needed from RED DA Inquire. This document will pull from your OMPF which make it official and can be printed. If document is not in your OMPF then the transaction may have failed; your will get an email notification from NSIPS if the transaction failed to be applied to your OMPF.

Other Co-Related Actions Reminder

- If your dependency status has changed (Add, Modified, Divorced or Deceased); ensure you take your supporting documentation **within 30 days from updating your RED DA application to RAPID office** (ID Card Labs) and they will update the DEERS system to reflect those changes. DEERS provides:
  - ID Card Issuance
  - Base access
  - Commissary & Exchange Privileges
  - Medical Benefits (Entitlement)
  - MIL-to-MIL are required to update DEERS to reflect MIL-to-MIL Spouse information in DEERS
- Don't forget to also **update your SGLI and FSGLI** to any changes you want reflected. Website can be accessed via My Navy Portal: https://my.navy.mil and selecting the milConnect tab, and once logged into milConnect, then select the "SOES" option under the "Benefits" tab. Access requires a Common Access Card, DFAS (myPay) account, or DS LOGON account. (See NAVADMIN 85/17 for more detail information). Additional URL sites:
- http://www.benefits.va.gov/insurance/docs/SOESContact.pdf
- http://www.benefits.va.gov/INSURANCE/training/SOES/SOES.htm
- http://www.public.navy.mil/bupers-npc/reference/messages/Documents/NAVADMINS/NAV2017/NAV17085.txt

DEERs/RAPIDS ID Card Issuance for ICAT 21 Dependents

- **DEERS/RAPIDS ICAT 21 – Dependents:**
- Dependents (children) are only authorized to carry Tri-Care prime under the sponsor until the age of 21 unless a full time student enrolled in an accredited college. If they are enrolled, they are eligible to maintain Tri-Care prime until the age of 23 or graduation (whichever comes first) .
- After the age of 23, the child is eligible for **Tri-Care Young Adult** (TYA) for a monthly premium.
- If they choose not to enroll in college as a full time student, they still may enroll in TYA from the age of 21-26 for the monthly premium
- **This premium ranges from $286 to over $300 a month pending on if the sponsor/dependent selects prime or standard**
- TYA, the dependent does NOT have privileges (commissary, exchange and MWR) they only receive medical coverage if SM elects TYA coverage.
- They are eligible to maintain TYA until the age of 26 or until they are married and no longer categorized a dependent of the sponsor.
- TYA does require 2 months premium up front to start the enrollment. Once this is paid, the ID card will be available immediately; HOWEVER, this still will require the sponsor to fill out the DD1172-2 authorizing issuance of the ID every time the dependent needs a new/replacement ID card because they are still a dependent of the sponsor.
- The PERM INCAP gets an indefinite ID card like the retirees and if the military member is Active Duty it's four year or until their EAOS or retirement. They lose all benefits if member is not providing over 50% support, the dependent get married or pass away
- DMDC's website for further information on the topic of children and benefits: https://milconnect.dmdc.osd.mil/milconnect/public/faq/Life_Events-Children/TyaNotAuto

RED DA Points of Contact Support

- **RED/DA Points of Contact:**
  - **NSIPS Helpdesk To Report Application Problems and Support**
    - NSIPS Help Desk for System Access or Report software issues by Opening a Trouble Ticket. Toll Free: 1-877-589-5991 DSN: 647-5442 Email: nsipshelpdesk@navy.mil
  - Contact your Command Pay and Personnel Administrator (CPPA) for training and assistance
  - Contact your Personnel Support Detachment for pending DA transaction or when Failed transaction support is needed.
  - **DA Support**
    - Mr. John Courtney PERS-2 (901) 874-2231 DA Support Email: john.g.courtney@navy.mil
  - **RED Support**
    - Mr. Al Gorski PERS-13 (901) 874-4559 RED Support Email: alan.gorski@navy.mil
  - **OMPF Support**
    - Mr. Jim Giger PERS-313 (901) 874-3406 OMPF Support Email: jim.giger@navy.mil
  - **Implementation Training and Support Leads**
    - **PSC Steven Roettger CNRFC (757) 322-5689 Email: steven.roettger@navy.mil**
    - **Mr. John Courtney PERS-22 (901) 874-2231 email: john.g.courtney@navy.mil**

QUESTIONS

First time RED/DA Users (Self-Service, CPC, PERS Clerk & PERS Supervisor) should follow these guidelines in order to successfully process transactions in RED DA. Failure to follow these guidelines will lead to failures for one or both transactions when submitting to EMPRS Lifecycle BOL.

Instructions:
For computers with Adobe Reader DC (new Software pushed from NMCI), open any Adobe document and ensure the correct settings for the digital signature are applied before proceeding below.
SOP for configuring Adobe settings can be found on the PERS-2 portal:
https://mpte.navy.deps.mil/sites/npc/pers2/RED%20DA/Forms/AllItems.aspx

For all of the available User Roles in RED DA, users should read and follow instructions to ensure desktop settings are correct (Adobe settings must also be updated). Remember, you should NOT print any document while in the process of completing your RED and/or DA forms. **Printing of the NAVPERS 1070/602 or DD Form 93 should only occur from RED DA Inquire after the PERS Supervisor approves and submits the application.**

1. Configure Compatibility View Setting using the step-by-step screenshots provided on the PERS-2 portal: https://mpte.navy.deps.mil/sites/npc/pers2/RED%20DA/Forms/AllItems.aspx

2. Next, clear the Cache using the step-by-step screenshots provided on the PERS-2 portal:
https://mpte.navy.deps.mil/sites/npc/pers2/RED%20DA/Forms/AllItems.aspx

3. Open any Adobe document and follow the step-by-step screenshots provided on the PERS-2 portal to ensure the Adobe digital signature settings are correct on the desktop.
https://mpte.navy.deps.mil/sites/npc/pers2/RED%20DA/Forms/AllItems.aspx

4. Close IE Browser windows and open a new one.

5. Now reboot your computer if you still have problems performing a RED DA transaction.

6. If you are still not able to digital sign any adobe documents contact your support helpdesk (NMCI, ONENET, MAIL.MIL, Marine Corp or other base service provider)

7. Go to NSIPS and log into Self-Service account at https://nsipsprod.nmci.navy.mil/

RED/DA Inquire is the ONLY place to print completed forms! Printing instructions are available on the PERS-2 portal: https://mpte.navy.deps.mil/sites/npc/pers2/RED%20DA/Forms/AllItems.aspx
"Do NOT print from any other location or the transaction will FAIL as the form believes changes were made to the Adobe document"
**Every Service Member in your command should ensure Internet Explorer and Adobe Reader DC settings are set before doing anything in NSIPS RED/DA application to avoid failures from occurring in EMPRS Lifecycle (BOL).

Please have the below Service Member(s) take action to resubmit their RED only as it failed at EMPRS Lifecycle; CPC's should only be concerned with the Service Member(s) that belong to their UICs:

NAME	DEPTID (Command UIC)	PSD

Instructions:
For computers with Adobe Reader DC (new Software pushed from NMCI), open any Adobe document and ensure the correct settings for the digital signature are applied before proceeding below.
SOP for configuring Adobe setting can be found on the PERS-2 portal:
https://mpte.navy.deps.mil/sites/npc/pers2/RED%20DA/Forms/AllItems.aspx

Service Member and PERS Supervisor should complete the below steps to ensure desktop settings are correct (Adobe settings must also be updated). After settings are updated by all users, the Service Member should complete Steps 7 – 16 below. If desktop settings are not set, begin with Step 1. Remember, you should NOT print any document while in the process of completing RED and/or DA forms. **Printing of the NAVPERS 1070/602 should only occur from RED DA Inquire AFTER the PERS Supervisor approves and submits the application.**

*1. Configure Compatibility View Setting using the step-by-step screenshots provided on the PERS-2 portal: https://mpte.navy.deps.mil/sites/npc/pers2/RED%20DA/Forms/AllItems.aspx

*2. Next, clear the Cache using the step-by-step screenshots provided on the PERS-2 portal: https://mpte.navy.deps.mil/sites/npc/pers2/RED%20DA/Forms/AllItems.aspx

*3. Open any Adobe document and follow the step-by-step screenshots provided on the PERS-2 portal to ensure the Adobe digital signature settings are correct on the desktop. https://mpte.navy.deps.mil/sites/npc/pers2/RED%20DA/Forms/AllItems.aspx

4. Close all IE Browser windows and open a new one.

5. Go to NSIPS and log into Self-Service account at https://nsipsprod.nmci.navy.mil/

6. Click RED DA Start Page.

7. Click Attachments and Remarks.

8. In Remarks: RED DD 93 (Service Member Only) Forms Block 14: member should type 'Resubmitted'.

9. Go to the Summary tab.

10. In the Forms area under DD Form 93, the Service Member should see "Signature Required".

11. Click on DD Form 93 and open the form.

12. Digitally sign the form and wait for the signature verification process to be applied (ensure a blue or black ribbon is displayed at the top left of the form). "**Do Not Print the Document**"

13. Click the Submit button in the form and follow the instructions which will take the Service Member back to the Summary tab in NSIPS.

14. Click Submit button in the Summary tab. Transaction will be routed to the supporting PSD for approval and release.

15. After the application has been approved and submitted by the PERS Supervisor, a printed copy can be obtained using the **RED DA Inquire** link by the Service Member (via ESR Self-Service), CPC (via Command RED DA User Role), or PERS Clerk/PERS Supervisor.

RED DA Inquire is the ONLY place to print completed forms! Printing instructions are available on the PERS-2 portal: https://mpte.navy.deps.mil/sites/npc/pers2/RED%20DA/Forms/AllItems.aspx

"Do NOT print from any other location or the transaction will FAIL as the form believes changes were made to the Adobe document if printed prior to submission to the OMPF"

**Every Service Member in your command should ensure Internet Explorer and Adobe Reader DC settings are set before doing anything in NSIPS RED/DA application to avoid failures from occurring in EMPRS Lifecycle (BOL).

Please have the below Service Member(s) take action to resubmit their DA only as it failed at EMPRS Lifecycle; CPC's should only be concerned with the Service Member(s) that belong to their UICs:

NAME	DEPTID (Command UIC)	PSD	Supervisor ID

Instructions:
For computers with Adobe Reader DC (new software pushed from NMCI), open any Adobe document and ensure the correct settings for the digital signature are applied before proceeding below.
SOP can be found on the PERS-2 portal:
https://mpte.navy.deps.mil/sites/npc/pers2/RED%20DA/Forms/AllItems.aspx

Service Member and PERS Supervisor should complete the below steps to ensure desktop settings are correct (Adobe settings must also be updated). After settings are updated by all users, the Service Member should complete Steps 7 – 16 below. If desktop settings are not set, begin with Step 1. Remember, you should NOT print any document while in the process of completing RED and/or DA forms. **Printing of the NAVPERS 1070/602 should only occur from RED DA Inquire AFTER the PERS Supervisor approves and submits the application.**

1. Configure the Compatibility View Setting using the step-by-step screenshots provided on the PERS-2 portal: **https://mpte.navy.deps.mil/sites/npc/pers2/RED%20DA/Forms/AllItems.aspx**

2. Next, clear the Cache using the step-by-step screenshots provided on the PERS-2 portal: **https://mpte.navy.deps.mil/sites/npc/pers2/RED%20DA/Forms/AllItems.aspx**

3. Open any Adobe document and follow the step-by-step screenshots provided on the PERS-2 portal to ensure the Adobe digital signature settings are correct on the desktop.
https://mpte.navy.deps.mil/sites/npc/pers2/RED%20DA/Forms/AllItems.aspx

4. Close all IE Browser windows and open a new one.

5. Go to NSIPS and log into Self-Service account at **https://nsipsprod.nmci.navy.mil/**

6. Click RED DA Start Page.

7. Click Attachments and Remarks.

8. In Remarks: DA NAVPERS 1070/602 (Service Member Only) Forms Block 46: member should type "Resubmitted".

9. Go to the Summary tab.

10. In the Forms area under NAVPERS 1070/602, the Service Member should see "Signature Required".

11. Click on NAVPERS 1070/602 and open the form.

12. Digitally sign the form and wait for the signature verification process to be applied (ensure a blue or black ribbon is displayed at the top left of the form). "**Do Not Print the Document**"

13. Click the Submit button in the form and follow the instructions which will take the Service Member back to the Summary tab in NSIPS.

14. Click the Submit button in the Summary tab. Transaction will be routed to the supporting PSD for approval and release.

15. PERS Supervisors taking final action on any DA form when applying digital signatures as the Authorizing Official must follow established work-around procedure. SOP is available on the PERS-2 portal: **https://mpte.navy.deps.mil/sites/npc/pers2/RED%20DA/Forms/AllItems.aspx**
Any deviation from the established work-around will cause the transaction to FAIL at EMPRS Lifecycle.

16. After the application has been approved and submitted by the PERS Supervisor, a printed copy can be obtained using the **RED DA Inquire** link by the Service Member (via ESR Self-Service), CPC (via Command RED DA User Role), or PERS Clerk/PERS Supervisor.

RED DA Inquire is the ONLY place to print completed forms! Printing instructions are available on the PERS-2 portal: **https://mpte.navy.deps.mil/sites/npc/pers2/RED%20DA/Forms/AllItems.aspx**

"Do NOT print from any other location or the transaction will FAIL as the form believes changes were made to the Adobe document if printed prior to submission to the OMPF"

**Every Service Member in your command should ensure Internet Explorer and Adobe Reader DC setting are set before doing anything in the NSIPS RED/DA application to avoid failures from occurring in EMPRS Lifecycle (BOL).

Information Paper:

Accessing "Travel Card Program" Training

DEFENSE TRAVEL MANAGEMENT OFFICE

Introduction

The DTMO-sponsored Travel Card Program course covers the basics about the Government Travel Charge Card (GTCC) program. The course provides information on obtaining, using, and paying balances on the GTCC, and is mandatory for all persons who have one. The course is approximately 75 minutes in duration.

Access and Login

To access the course, navigate to Passport at https://www.defensetravel.dod.mil/passport (Figure 1). You will need to have a user account to login to Passport. If you do not have an account, you may create one by selecting the **Register** button, complete then submit the form.

Figure 1: DTMO Passport Account Login

TURN OFF POP-UP BLOCKER

TraX

The DoD Travel Explorer Home page displays (Figure 2). Navigate to the Training courses by selecting the **Training** icon.

Figure 2: DoD Travel Explorer Home Page

This document is controlled and maintained on the www defensetravel dod mil website. Printed copies may be obsolete.
Please check revision currency on the web prior to use

The Training section of TraX lists courses that support your role (Figure 3). To see the Travel Card course in the list of available classes, you will need to complete the **My Roles** tab.

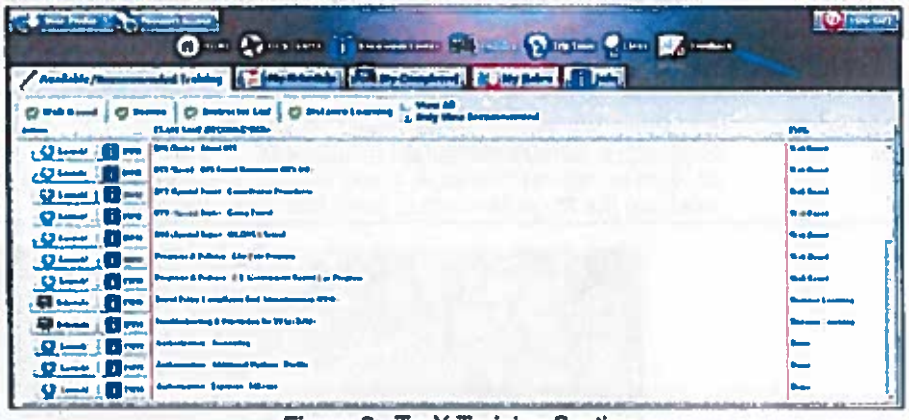


Figure 3: TraX Training Section

Place a check in the box next to **I am a DoD Traveler and/or I use DTS** or in the box next to **I have a Travel Card.** After selecting the applicable roles, select **View Recommended Training** (Figure 4).

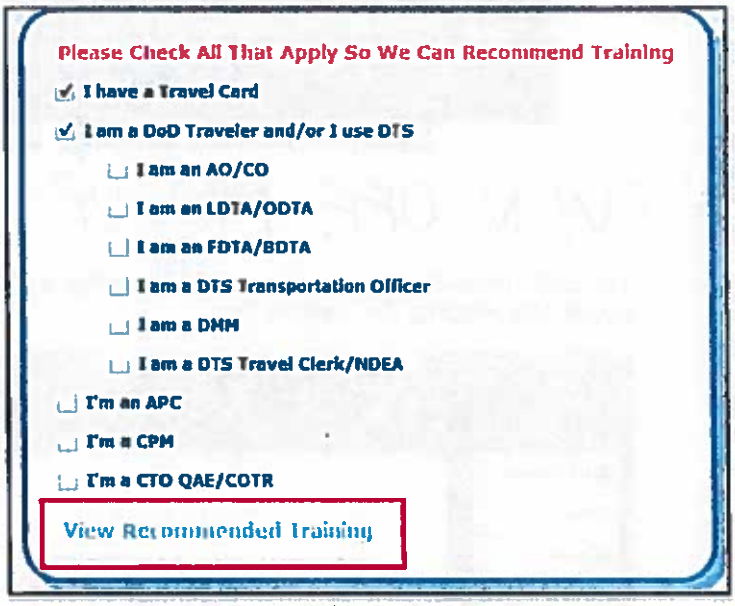


Figure 4: My Roles Section

Launching the Course

The screen returns to the Available/Recommended Training tab, and the Travel Card course displays in the list. (If you still don't see the course on the list, select the "View All" radio button).Start the course by selecting **Launch** to the left of the course titled: **Programs & Policies-Travel Card Program (Travel Card 101) [Mandatory]** (Figure 5).

This document is controlled and maintained on the www.defensetravel.dod.mil website. Printed copies may be obsolete. Please check revision currency on the web prior to use.

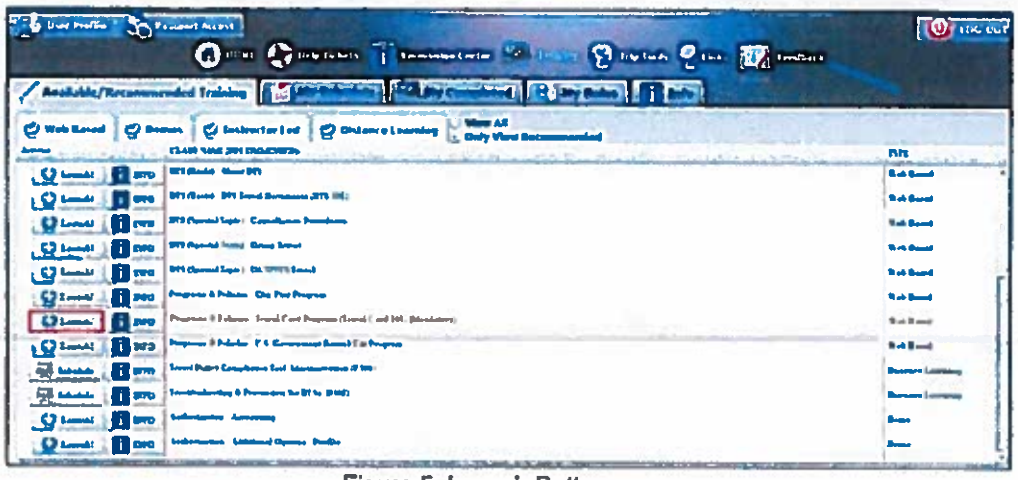


Figure 5: Launch Button

Another browser window opens with a screen providing information about the system requirements for accessing the training. When you have verified that your computer is properly equipped and the settings are properly configured, select **Launch Course** either at the top or the bottom of the window (Figure 6).

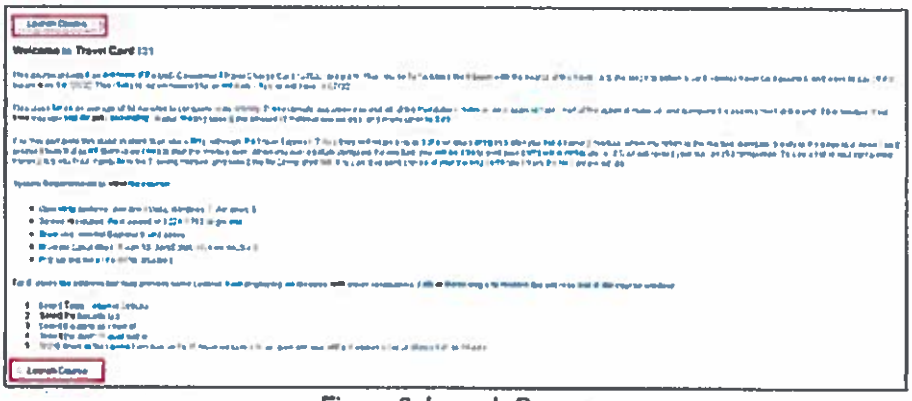


Figure 6: Launch Course

The Launch screen of the Travel Card course appears.

This document is controlled and maintained on the www.defensetravel.dod.mil website. Printed copies may be obsolete.
Please check revision currency on the web prior to use.

Individually Billed Account Travel Card Set Up Form

Citibank® Government Travel Card Program

Hold off on Item 11

Instructions:

This form must be completed by the Department of Defense employee, approving supervisor and the Agency Program Coordinator (APC). Use this form to apply for a new Individually Billed Card Account to be used by a Department of Defense employee. Information collected on this application is subject to the Privacy Act of 1974 (5 U.S.C. 552a) and applicable agency regulations. Questions? Contact Commercial Card Services toll-free 1-800-200-7056 from the U.S. and Canada or, if dialing from international locations, call collect 757-852-9076. ***See pages 3-5 for detailed instructions on completing this form.***

Section I: Reporting Parameters *(To be completed by APC. * = Required fields)*

1. Citi Account Hierarchy*	Specify the complete 5-digit account Hierarchy Level (HL) numbers that pertain to your organization. Each Hierarchy Level consists of 5 digits.						
	HL1	HL2	HL3	HL4	HL5	HL6	HL7

Section II: Cardholder Information *(To be completed by employee. * = Required fields)*

2. Applicant Name*	Provide full name: First, Middle Initial and Last name of the applicant as it should appear on the card *(maximum of 24 characters – including spaces)*			
3. Applicant SSN*	- -		4. Date of Birth (mm/dd/yyyy)*	/ /
5. Applicant Address Details*	*Address must be U.S., U.S. territory, APO/FPO/DPO. Application will not be processed if a foreign address is provided.* *If your Primary Address is a P.O. Box or if your Card should be shipped to an Alternate Address, please complete the Alternate Address section below. Applications providing only a P.O. Box will not be processed; a physical address is required. For APO/FPO/DPO addresses only, an Alternate/physical Address is not required. For Expedited Card Delivery a physical address is required.* ☐ **Expedited Card Delivery** (Note: A $20 fee will be charged) ☐ **Ship Card to Alternate/Physical Address**			
	Primary Address* (this is where your statement will be mailed)		Alternate/Physical Mailing Address* (No Post Office Box)	
	Mail to Attention		Mail to Attention	
	Address Line 1*		Address Line 1*	
	Address Line 2		Address Line 2	
	City or APO/FPO*		City or APO/FPO*	
	State*	Zip/Postal Code*	State*	Zip/Postal Code*
6. Applicant Contact Details*	E-mail Address*		Home Phone* ( )	
	Commercial Office Phone* ( )		Cell Phone ( )	
7. Employee ID	*10 digit number found on the back of the DoD issued CAC card.*			

Section IIa: Cardholder Information *(To be completed by employee.)*

8. Paper-free Option	You have the option to receive your card account billing statement ("statement") electronically and certain notices, including legal notices, for your card account ("notices") electronically. If you select this option, your statement as well as any notices that we make available electronically now or in the future will be available to you for viewing on the CitiManager web site and will not be mailed to you, and we will send you an e-mail alert to the e-mail address provided above when your statement or a notice is ready for viewing. If you wish to select this option, please check the box below. ☐ By checking this box, I agree to receive statements and notices electronically as described above and to receive e-mail alerts of statements and notices. I understand that I must register for CitiManager at www.citimanager.com/login in order to view statements and notices electronically.

© 2017 Citibank, N.A. All rights reserved. Citi and Arc Design is a registered service mark of Citigroup Inc.

Individually Billed Account Travel Card Set Up Form

Citibank® Government Travel Card Program

Section III: Cardholder Signature & Agreement *(To be completed by employee. * = Required fields)*

Signature & Agreement*	By signing below, I: (i) acknowledge I have read the Citi® Department of Defense Services Travel Card Program *Cardholder Agreement*; (ii) agree to be bound by the terms and conditions as set forth in the Agreement, and (iii) understand that only the Department of Defense may request particular Authorization Parameters (Section III). This application is for a Department of Defense Travel Card account, which may be standard or restricted, as described in the Cardholder Agreement. I expressly agree to accept whichever type of account is established. Pursuant to requirements of law, including the U.S.A. PATRIOT ACT, the bank is required to request additional information to verify your identity. *IMPORTANT INFORMATION about opening a new Citibank® Corporate Travel Card account: To help the United States Government fight terrorism and money laundering, Federal law requires us or your employer to obtain, verify, and record information that identifies each person that opens an account. What this means for you: when you open an account, we or your employer will ask for your name, a street address, date of birth, and an identification number, such as a Social Security number, that Federal law requires us or your employer to obtain. We or your employer may also ask to see your driver's license or other identifying documents that will allow us or your employer identifies you. We appreciate your cooperation.*		
	9. Applicant's Signature*		**10. Date***
	11. Credit Report Authorization* (initial one)	A. _____ I, as the cardholder, authorize the bank to obtain credit reports on me as described in the agreement.	B. _____ I, as the cardholder, DO NOT authorize the bank to obtain credit reports on me. Therefore, I will not be eligible for a standard card.
	12. Approving Supervisor's Signature*		13. Date*

Section IV: Account Specification *(To be completed by APC. * = Required fields)*

14. ☐ Restricted by APC (See detailed instructions pages 2-4)	
a) Date to Activate (mm/dd/yyyy)	b) Date to Deactivate (mm/dd/yyyy)

Section V: Authorization *(To be completed by APC. * = Required fields)*

15. Authorized APC*	By signing below, I hereby authorize, on behalf of the Agency/Organization indicated above, that a Department of Defense Travel Card be issued to the employee named in Section I of this application. PLEASE RETAIN A COPY FOR YOUR RECORDS.			
	APC Name (type or print)*	VANESSA N. READO	E-mail Address*	vanessa.reado@navy.mil
	APC Signature*		Date*	
	Commercial Office Phone*	(850) 452-2907		

© 2017 Citibank, N.A. All rights reserved. Citi and Arc Design is a registered service mark of Citigroup Inc.

DEFENSE TRAVEL MANAGEMENT OFFICE

June 2016

STATEMENT OF UNDERSTANDING (SOU)

The Government Travel Charge Card (GTCC) is mandated to be used by DoD personnel to pay for authorized expenses when on official travel unless an exemption is granted. This includes temporary duty travel (TDY), and, per Component guidance, permanent change of station (PCS) travel.

Cardholder must check off each item below.

I understand that I am being directed to:

(PLEASE CHECK OFF EACH BOX)

- ☐ Use my card only for expenses incurred by me for official travel, and my dependents, if authorized for PCS travel.
- ☐ Confirm receipt of my GTCC upon delivery.
- ☐ Ensure that my card is activated by my APC before I travel.
- ☐ Pay all my undisputed charges by the due date on my billing statement, regardless if my travel voucher has been processed.
- ☐ Use split disbursement to pay for all outstanding charges.
- ☐ 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 business days after completing my travel.
- ☐ Obtain tax exemption information prior to my trip from https://smartpay.gsa.gov/content/state-tax-information.
- ☐ Keep my account number, expiration date and contact information updated in DTS.
- ☐ Update my contact information with the travel card vendor, when necessary.
- ☐ Notify the travel card vendor, and my APC, if my GTCC is lost or stolen.
- ☐ 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 submitted within 60 calendar days from the statement date.
- ☐ 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.

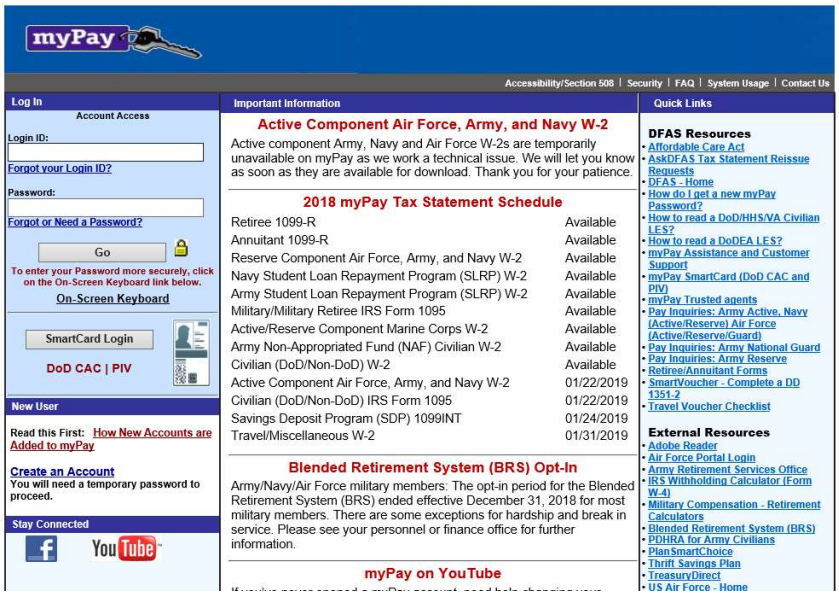
For additional information on the Travel Card, refer to your APC and the DoD GTCC Regulations (http://www.defensetravel.dod.mil/Docs/regulations/GTCC.pdf).

APC's Name: _____ APC's Phone Number: _____

_____	_____	_____
Applicant Name/Signature	Date	Supervisor Name/Signature

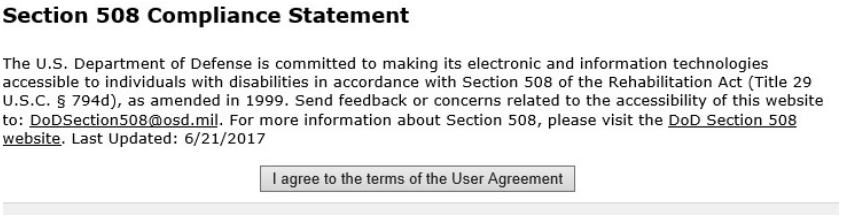
My Pay via Defense Finance and Accounting Service (DFAS)

https://mypay.dfas.mil/mypay.aspx

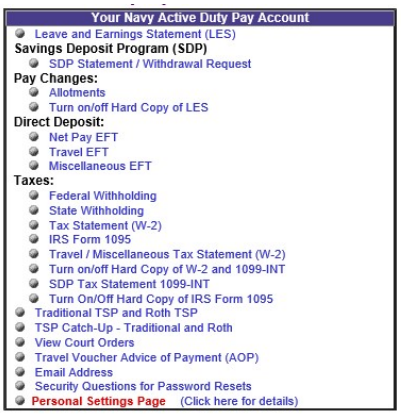


Proceed to MyPay website and select Create Account for New User, Smart Card Login with CAC Reader or use the Login ID and Password you created.

If you created a new account return to home page and login.



Scroll to bottom of page and select “I agree”.



Select Leave and Earnings Statement (LES)

Select pay period from drop down menu.

DEFENSE FINANCE AND ACCOUNTING SERVICE MILITARY LEAVE AND EARNINGS STATEMENT

ID	NAME (Last, First, MI)	SOC. SEC. NO.	GRADE	PAY DATE	YRS SVC	ETS	BRANCH	ADSN/DSSN	PERIOD COVERED
									1-31 DEC 18

ENTITLEMENTS

	Type	Amount
A	BASE PAY	
B	BAS	
C	BAH	
D	FLY PAY	
E		
F		
G		
H		
I		
J		
K		
L		
M		
N		
O		
	TOTAL	8767.46

DEDUCTIONS

Type	Amount
FEDERAL TAXES	
FICA-SOC SECURITY	
FICA-MEDICARE	
	4888.04

ALLOTMENTS

Type	Amount
	11.39

SUMMARY

+Amt Fwd	.00
+Tot Ent	
-Tot Ded	
-Tot Allt	
=Net Amt	
-Cr Fwd	
=EOM Pay	

DIEMS	RETPLAN

LEAVE	BF Bal	Emd	Used	Cr Bal	ETS Bal	Lv Lost	Lv Paid	Use/Lose
			0		.0	.0	.0	.0

FED TAXES	Wage Period	Wage YTD	M/S	Ex	Add'l Tax	Tax YTD
				--	.00	

FICA TAXES	Wage Period	Soc Wage YTD	Soc Tax YTD	Med Wage YTD	Med Tax YTD

STATE TAXES		Wage Period	Wage YTD	M/S	Ex	Tax YTD

PAY DATA	BAQ Type	BAQ Depn	VHA Zip	Rent Amt	Share	Stat	JFTR	Depns	2D JFTR	BAS Type	Charity YTD	TPC	PACIDN

TRADITIONAL PLAN (TSP)	Base Pay Rate	Base Pay Current	Spec Pay Rate	Spec Pay Current	Inc Pay Rate	Inc Pay Current	Bonus Pay Rate	Bonus Pay Current
ROTH PLAN	Base Pay Rate	Base Pay Current	Spec Pay Rate	Spec Pay Current	Inc Pay Rate	Inc Pay Current	Bonus Pay Rate	Bonus Pay Current

CM AGCY CONTR	AGCY-AUTO	AGCY-MATCH				
CONTRIBUTIONS TOTALS	YTD Deductions	YTD TSP Deferred	YTD TSP Exempt	YTD ROTH	YTD TSP AGCY-AUTO	YTD TSP AGCY-MATCH

REMARKS: YTD ENTITLE _____ YTD DEDUCT _____

WWW.DFAS.MIL

DFAS Form 702, Jan 02

Leave Balance

BAH if married ensure it reads "W/DEP"

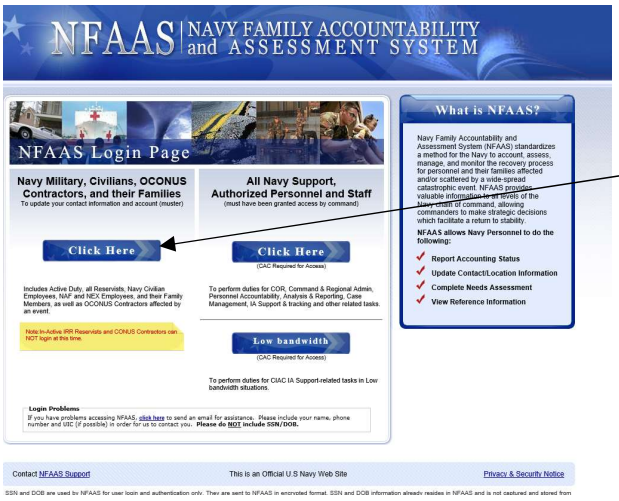
Read the Remarks!

Pay Period being viewed.

Retirement Information

Navy Family Accountability and Assessment System (NFAAS)

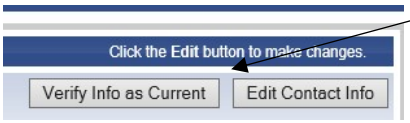
https://navyfamily.navy.mil/cas/login?service=https%3A%2F%2Fnavyfamily.navy.mil%2F



Proceed to NFAAS website and select Navy Military Login.

Login with CAC Card.

Select each menu item to view information.



Verify or Edit with Updated information.

DEPARTMENT OF THE NAVY
CHIEF OF NAVAL AIR TRAINING
250 LEXINGTON BLVD SUITE 102
CORPUS CHRISTI TX 78419-5041

29 Jan 19

MEMORANDUM FOR DISTRIBUTION

From: Chief of Naval Air Training

To: All Hands

Subj: COMMON ACCESS CARD AND PERSONAL ELECTRONIC DEVICE REQUIREMENTS FOR CHIEF OF NAVAL AIR TRAINING AND SUBORDINATE COMMANDS

1. All CNATRA and NATRACOM Personnel (Military, Civilians, and Contractors) will adhere to Cyber Security policies, directives and best practices at all times. If you notice an unattended Common Access Card (CAC) you are not allowed to remove it. Contact the Military Member/Employee's Supervisor and the responsible Command Security Manager immediately.

Actions you should take to safeguard your CAC:

a. Maintain control of your CAC/Military Identification (ID) at all times.

b. Remember to remove your CAC from your computer when you leave your desk.

c. Do not display your CAC or any other credentials that contain Personally Identifiable Information (PII) when you leave the workplace. For example, do not have your CAC/Military ID visible while riding public transportation.

d. Except for Department of Defense (DoD) health care providers, do not allow organizations/businesses to reproduce (photocopy, scan, or other means) an image copy of your CAC/Military ID. If you know of a non-medical organization possessing an image copy of your CAC/Military ID, request destruction of the image.

e. In the event a CAC scan application comes into the market, do not attempt to use or test it on your mobile device, as the barcode information may be sent to an unknown server, stored, and made available for public release.

2. Personal Electronic Devices (PEDs) are not allowed for official business. All CNATRA and NATRACOM personnel are required to use government provided email, mobile devices and computer hardware/software for official business. Use of commercial email (Yahoo, Gmail, etc.) may only be used in the event government provided services are not available and must be authorized in writing by the first Flag Officer in the Chain of Command. PEDs are not authorized to be connected to government computer systems. Unauthorized devices are detected by automated computer security systems. These connections are blocked, but will trigger a computer security incident.

3. Cyber Security is everyone's responsibility. Unit Commanders are directed to brief this information to all hands immediately and implement measures to ensure 100% compliance with all DoD/Department of the Navy (DON) policies and directives.

G. N. HARRIS

Copy to:
CNATRA Website

(13)

CNATRA CYBERSECURITY

Security

The protection of Government assets, people and property, both classified and controlled unclassified, is the responsibility of each and every member of the Department of Defense, regardless of how it was obtained or what form it takes. Our vigilance is imperative in the protection of this information. Anyone with access to these resources has an obligation to protect it.

The very nature of our jobs dictates we lead the way in sound security practices. Anything less is simply not acceptable.

Physical and cyber security is a team effort. Your diligence in promptly reporting concerns and adhering to your agency's security policies and procedures will ensure the integrity of national security. As a team, we can protect our warfighters, colleagues, and families from potential harm.

DoD IA Responsibilities

In the performance of your duties you are required to have access to government information systems.

Information assurance protects and defends information and information systems by ensuring their availability, integrity, and confidentiality.

DoD IA Responsibilities

- Participate in annual IA training inclusive of threat identification, physical security, acceptable use policies, malicious content and logic, and non-standard threats such as social engineering.

- Comply with password or pass-phrase policy directives and protect passwords from disclosure.

- Complete a SAAR and End User Agreement at every command indoc or at least every 3 years.

- Annual OPSEC/Counter Intelligence briefing.

CAC

- Maintain control of your CAC/Military ID at all times. IAW DODI 1000.13 "An ID card shall be in the personal custody of the individual to whom it was issued at all times. If required by military authority, it shall be surrendered for ID or investigation."

- Remember to remove your CAC from your computer when not physically present at your desk.

- Do not display your CAC or any other credentials that contain Personally Identifiable Information (PII) when you leave the workplace.

- Do not use unapproved CAC scan applications. Barcode information may be compromised.

CAC

Information Stored on a CAC

- Name
- Date of birth
- Personnel category
- Pay category
- Benefits information
- Organizational affiliation
- Pay grade
- Two digital fingerprints
- Digital photo
- Organizational affiliation
- Agency
- Department
- Expiration date
- Public Key Infrastructure (PKI) certificates that enable cardholders to "sign" documents digitally, encrypt and decrypt emails, and establish secure online network connections.

CAC

Non-Repudiation and your CAC

Digital signatures provide authentication for applications such as email. These digital signatures also provide non-repudiation. A user cannot later deny malicious acts because their CAC provided their digital signature even when used by someone else.

Digital audit logs also record details about actions taken while using your digital signature. If there are malicious acts to the network, files, etc., you will be held responsible.

You wouldn't leave the keys to your house in your front door, or your ATM card in the machine. Treat your CAC with the same care to protect yourself.

Unauthorized Devices

Use of unapproved devices to process non-publicly releasable data increases the risk to the network. Devices attached to or inserted into the end point's plug-and-play ports and slots can be a vector for the insertion of malware when used to access the network.

Storage devices are portable and can be easily concealed. Devices with volatile memory (erased when not connected) may contain internal batteries that also pose a threat to attached systems. Requiring approval prior to use of these devices heightens awareness of the threat, limits the potential use of contaminated devices, and allows for proper tracking and control.

Designated Approval Authority (DAA) approval of flash memory devices is required by the United States Cyber Command (USCYBERCOM) Communications Task Order (CTO) 10-084 Removable Flash Media Device Implementation within and between Department of Defense (DoD) Networks (U/FOUO) (or latest version of this CTO).

Unauthorized Devices

CNATRA Policy prohibits use of Personal Electronic Devices (PEDs) for official business. You must use government provided email, mobile devices and computer hardware/software for official business.

Unauthorized devices are not allowed to be connected to information systems. Connections are blocked but will trigger a security incident. Violators will temporarily lose access privileges and be required to complete Information Assurance training, complete a new SAAR, submit a statement and complete counseling.

Spot Checks/Inspections

CNATRA Policy requires periodic security spot checks for all commands. These spot checks can be completed by, ISSO's, Security Managers, or by a Department Head.

All spot checks will be documented and tracked. Results for the checks, and any required remediation for failures will be reported up to CNATRA.

All first time violations will require a completion of Information Awareness Training and documented counseling from the supervisor no later than 5 days after the finding. Second time violations may result in suspension from the DOD information network for a specified period of time.

Repeated violations or willful disregard of regulations will result in formal reporting to DOD Central Adjudication Facility for record and reevaluation of your clearance.

Violations

Violation of the policies associated with security policy may result in disciplinary action at the discretion of an individual employee's supervisor(s) and/or senior executive management chain.

(1) Department of Defense (DoD) civilian, military, and contractor employees will potentially be subject to various levels of sanctioning (e.g., warning, reprimand, suspension without pay, forfeiture of pay, removal, discharge, loss or denial of access to classified information, removal of classification authority, termination of employment) if they knowingly, willfully, or negligently compromise or place CNATRA information systems and/or sensitive information at risk of compromise.

(2) Military Service members may be subject to administrative or disciplinary action as authorized by applicable regulations and the Uniform Code of Military Justice.

(3) Applicable Federal or state law(s), to include the Privacy Act, will be enforced. The Privacy Act authorizes civil and criminal penalties for violating certain provisions of the act.

CNATRA information system users must understand that they will be held accountable for their actions and are responsible for securing the data and resources in accordance CNATRA policies. By adhering to the these policies, users contribute greatly to the culture of a safe, secure, mission- oriented work environment for all CNATRA information system users.

ENCLOSURE 2 - Acceptable Use of DON IT
February 10, 2016

1. **General Use**

a. DON IT users are every Sailor, Marine, civilian, contract support person, or foreign national with approved access to DON IT.

b. DON IT users must observe all policies and procedures governing the secure operation and authorized use of DON IT.

c. Users of systems that impact financial statements will not only follow prescribed internal controls set by policies and procedures governing secure operation and authorized use of DON IT, they will also follow internal controls required per Federal Information System Control Audit Manual (FISCAM) audit methodology (available on the DON CIO web site: http://www.doncio.navy.mil}.

d. DON IT resources are provided for official use and authorized purposes only. Authorized purposes may include personal use within the limitations set forth in reference (d}. Personal use must not adversely affect the performance of official duties or degrade network performance, and must be of a reasonable duration and frequency as determined by commanding officers and supervisors. This includes personal communications from the DON IT users that are most reasonably made during the work day (such as checking in with spouse or minor children, scheduling doctor and auto or home repair appointments, brief Internet searches, emailing directions to visiting relatives, conducting on-line banking, distance learning, checking commercial email account, etc.). Nonemergency personal communications shall be made during personal time, such as after duty hours or lunch periods.

e. Users must not use DON IT to access inappropriate web sites or applications. Any questions regarding appropriateness of web sites or applications should be addressed to supervisors.

f. Users must not use DON IT in violation of the Hatch Act (5 U.S.C. §§ 7321-7326), which limits certain political activities of most federal executive branch civilian employees. Military personnel are similarly affected by Department of Defense Directive 1344.10, which mirrors the Hatch Act. The Hatch Act has a wide and evolving scope. Any questions regarding prohibited behaviors should be addressed to a supervisor or ethics officer. Below are some specific prohibitions; but not a comprehensive list. DON IT users must not:

(1) Engage in political activity while on duty or in the workplace. This includes partisan political social media posts, "likes," shares, pictures, "tweets," "re-tweets," and sending email messages and links, etc., even when using an alias, personal social media account, or personal email account.

(2) Send or forward partisan political communications via social media or email to a subordinate at any time.

(3) Engage in political activity in an official capacity at any time, or refer to official titles or positions while engaged in political activities. This includes using an official email account or a social media account created for use in an official capacity to engage in political activity.

(4) Suggest, solicit, or receive political contributions at any time. This includes sending or forwarding invitations to political fundraising events and providing links to partisan political contribution sites or pages.

(5) Forward partisan political emails received by a government account to anyone or any place other than their own personal email accounts.

g. DON IT users may not use official email addresses to sign up for non-official online services (e.g., adult content,)

h. Commands shall ensure required background investigations are completed commensurate with the level of DON IT access a user requires, per references (e) and (f).

i. All DON IT users shall have approved DON system authorization access requests (SAAR) on file prior to being granted access to DON networks.

j. DON IT users must not bypass, stress, or test cybersecurity (CS) or computer network defense (CND) mechanisms (e.g., firewalls, content filters, proxy servers, anti-virus programs).

k. Users must not introduce or use unauthorized software, firmware, or hardware on any DON IT resource.

l. Users must not relocate or change equipment or the network connectivity of equipment without authorization from the local CS authority (i.e., person responsible for the overall

implementation of CS at the command level, such as the Information System Security Manager).

m. Users must not use personally owned hardware, software, shareware, or public domain software for official DON business without written authorization from the local CS authority.

n. Users must not upload or download executable files (e.g., .exe, .com, .vbs, or .bat) onto DON IT resources without the written approval of the local CS authority.

o. Users must not use DON IT to participate in or contribute to any activity resulting in a disruption or denial of service.

p. Users must not use DON IT to write, develop, compile, store, transmit, transfer, or introduce unauthorized or malicious software, programs, or code.

q. In accordance with reference (d), users must not use DON IT resources in any way that would reflect poorly on the DON. Such uses include, but are not limited to, pornography, chain letters, unofficial advertising, soliciting or selling (except on authorized bulletin boards established for such use), violation of statute or regulation, inappropriate handling of classified information and Personally Identifiable Information (PII), and other uses that are incompatible with public service.

r. Users must follow the specific guidance provided in references (g) and (h) to properly safeguard controlled unclassified information (CUI), including PII and for official use only (FOUO).

s. Users must report all security incidents, including PII breaches, immediately in accordance with references (r), (s), (n) and Command policy and procedures.

t. Users must not place data onto DON IT resources whose security controls are insufficient to protect that data (i.e., data classified Secret may not be placed onto an unclassified network).

u. Users must protect DoD/DON information and IT to prevent unauthorized access, compromise, tampering, exploitation, unauthorized or inadvertent modification, disclosure, destruction, or misuse

v. Users must protect authenticators {e.g., passwords and personal identification numbers (PIN)) required for logon authentication at the same classification as the highest classification of the information accessed.

w. Users must protect authentication tokens (e.g., common access card (CAC), alternate logon token (ALT), personal identity verification (PIV), national security systems (NSS) tokens) at all times. Unattended tokens must be properly secured.

x. Users must virus-check all information, programs, and other files prior to uploading them onto any DON IT resource.

y. Users must access only that data, classified and unclassified controlled information, software, hardware, and firmware for which they are authorized access, have a need-to-know, and have the appropriate security clearance. Users must assume only those roles and privileges for which they are authorized.

z. Commanders of DON organizations shall obtain formal authorization to interconnect information systems and networks per references (e), (i), (j) and (k).

aa. DON organizations may use Internet based capabilities as defined in references (g), (h), (I) and other applicable policies.

bb. Commanders of DON organizations shall control the access of contractors and representatives of foreign nations, coalitions, or international organizations to DON IT and the information residing on those systems, in accordance with relevant national and DoD policies and guidance, including references (e), (f), (i), (j), (m), (n), (o), (p), and (q).

2. Training Requirements

a. Users must complete DoD approved CS courses within 30 days after receiving access to DON IT. Commanders of DON organizations may add specific DON, Service, and local CS policies and procedures. DoD CS training includes initial orientation and an annual refresher course. Completing the annual CS refresher course is a condition that users must meet for continued use of DON IT.

b. Users must complete personally identifiable information (PII) training annually.

c. DON IT users must complete derivative classification training prior to being granted initial access to DON classified IT and biennially thereafter.

3. Email Use

a. Users must digitally sign email messages requiring either message integrity or non-repudiation using DoD Public Key Infrastructure (PKI) or other approved method. All email containing an attachment or embedded active content must be digitally signed.

b. Users must encrypt CUI contained in email in accordance with reference (r). Examples of this are attachments that contain personal identity or budget information.

c. Use of commercial email for certain types of unclassified information for official government business is only permitted under the following conditions, and failure to comply may result in administrative or punitive action:

(1) Pre-approval requirements:

(a) To meet an urgent operational requirement(s) wherein the user will not have access to unclassified DON IT systems (e.g., NIPRNET). This method is not authorized as a routine means.

(b) User must submit a request in writing and have it approved by a FO/GO SES in the chain of command, prior to using commercial email. The request must include the urgent operational requirement(s) and validation of compliance with the requirements in subparagraph 2 and 3 below.

(c) FO/GO/SES personnel are considered sufficiently senior to pre-approve use of personal email when the conditions cited in 1 .a above apply. However, they must still ensure compliance with the requirements in subparagraphs 2 and 3 below.

(d) A copy of the approval must be provided to DUSN(P) Security for reference.

(2) Records generated:

(a) Once approval has been obtained per requirements in paragraph 1 above, DON personnel must include their official government email address on all email transmissions containing DON unclassified information. Transmitting DON unclassified information to any other commercial email address is prohibited.

(b) If unable to copy their official government email address, users must forward complete copies of the information to their official government email address within 20 days of the original creation or transmission of the record per reference (z) and 44 U.S.C. § 2911.

(3) Level of information authorized and prohibited:

(a) Authorized (only when digitally signed and encrypted per DoD Manual 5200.01-Volume 4):

1. Unclassified official government information that does not require safeguarding and dissemination controls, pursuant to and consistent with applicable law, regulations, and government-wide policies.
2. Unclassified//For Official Use Only (U//FOUO) information as defined in DoD Manual 5200.01-Volume4, which is a type of controlled unclassified information (CUI). This includes FOUO information that qualifies for protection pursuant to the provisions of the Privacy Act of 1974, as amended (i.e., Personally Identifiable Information (PII)).

(b) Prohibited:

1. Classified information.
2. All other current types of CUI outlined in DoD M-5200.01-Volume 4 and SECNA V M-5510.36, such as Department of State Sensitive But Unclassified, Drug Enforcement Administration Law Enforcement, Unclassified Naval Nuclear Propulsion Information, Unclassified Critical Nuclear Weapons Design Information, National Geospatial-Intelligence Agency unclassified imagery or geospatial information, unclassified Technical Documents with Distribution Statement F or X, etc.

d. Users must not auto-forward official email from their DON email accounts to commercial email accounts.

e. Commanders of DON organizations may authorize remote access via Outlook Web Access (OWA) to unclassified official email using personally owned and other non-DoD computers. Commanders and users must document the verifiable need, and ensure the approval; training, configuration, and process comply with DON and Service OWA policy.

(1) Users must:

(a) Submit a request/signed statement accepting responsibility for approved access for each computer expected to access email.

(b) Indicate a valid requirement (convenience alone is not a valid requirement)

(c) Use PKI authentication

(d) Handle, store, maintain and destroy all unclassified information in accordance with DoD and DON policies.

(e) Immediately notify their commands of any information loss, theft or suspicious behavior of their system(s).

(f) Protect the confidentiality, integrity and availability of DON e-mail systems and information at all times.

(g) Complete Service designed specific OWA training prior to accessing OWA.

(h) Install, configure, maintain and update required security software, hardware, PKI certificates and current anti-virus files by updating them at least weekly or when prompted.

(i) Not use public access computers, such as those in college computer labs, public kiosks, libraries, etc. to access DON or DoD unclassified e-mail accounts.

(j) Use Wireless Fidelity (WiFi) hotspots only if the connection and user complies with remote access requirements.

(k) Ensure that no other wireless or LAN connection exists for the duration of the OWA session. Any other existing connections must be disabled for the duration of the session.

(l) At the completion of an OWA session:

1. Close all DON email files;
2. Clear the web browser's cache;
3. Exit and close the browser; and
4. Immediately turn off the computer. "Sleep" and "standby" modes are not acceptable.

(2) Commanders of DON organizations must:
   (a) Document authorization to use OWA by name or command wide with an authorized users list; maintain the authorized users list.
   (b) Evaluate each request for validity and approve those essential for mission accomplishment.
   (c) Retain all user signed statements until that member's detachment from the command.
   (d) Review approvals annually.
   (e) Disable access immediately upon a member's detachment.
   (f) Conduct oversight for compliance and take appropriate actions for non-compliance.

4. Remote Access

a. Commanders of DON organizations shall control remote access to DON IT per references (e), (f), (i), (j), (m), (t), (u), and (v).

b. Commanders of DON organizations shall provide government-furnished computer equipment, software, and communications with appropriate security measures as the primary means for remote access for any regular and recurring telework arrangement that involves CUI information, per reference (w).

c. Commanders of DON organizations must ensure all remote access to DoD information systems and networks, including telework access, is mediated through a managed access control point, such as a remote access server in a DMZ. Use encryption to protect the confidentiality of the session, per reference (e).

d. Commanders of DON organizations must ensure authentication and confidentiality requirements for remote access sessions use National Security Agency (NSA)-approved COMSEC and keying material for classified systems and National Institute of Standards and Technology (NIST)-approved COMSEC and DoD PKI certificates for unclassified systems.

e. Commanders of DON organizations shall consider mandating the use of Virtual Private Networks (VPNs) to protect and control internal and external access to their information systems and networks, if a mission need for remote access is established. VPNs are the preferred method when using government-furnished or government-contracted equipment.

f. Commanders of DON organizations and users of DON IT must ensure all computers used for remote access have DoD approved antivirus and firewall protection that includes the capability for automated updates per references (e), (i), and (j). The most current definitions and updates for these applications must be loaded before a remote access session is established.

g. DON IT administrators /privileged users must comply with the following requirements when accessing DON IT from outside of the enclave:
   (1) Once the DON organization determines the mission need for remote access, they must establish approved VPN connections using government-furnished equipment under their user accounts (with user privileges). All remote access to DON classified systems or networks must use NSA-approved COMSEC and keying material.
   (2) After establishing a secure connection, elevate permissions to the appropriate level for conducting administrator tasks.
   (3) Terminate connection when administrator tasks are complete.
   (4) Safeguard intonation (i.e., do not access or display in an area where unauthorized persons are present) and control the equipment after connection termination per reference (x).

5. PKI Requirements

a. DON IT users must ensure encryption of CUI contained in Web server transactions using DoD PKI.

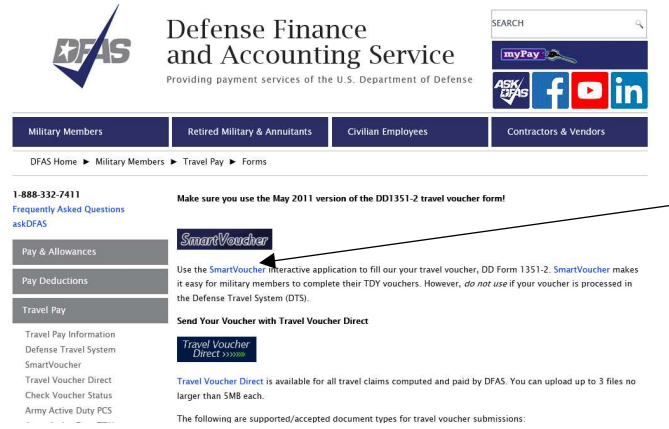
b. Users may only use software based certificates when the DON CIO or the appropriate DON Deputy CIO provides written certification of mission essentiality. This does not preclude the use of software certificates related to the DoD External Certificate Program, device/server software certificates, and software certificates used for group/role based functions.

c. General Officers/Flag Officers/Senior Executive Service members and their designated staff may use Alternate (ALT) tokens to maintain security and support senior level requirements. ALT tokens must be in accordance with the procedures in reference (y). Use of ALT tokens within the Secretariat staff must be approved by the DON CIO. The DON Deputy CIO (Navy) must approve their use by Navy staff, and the DON Deputy CIO (Marine Corps) for Marine Corps staff.

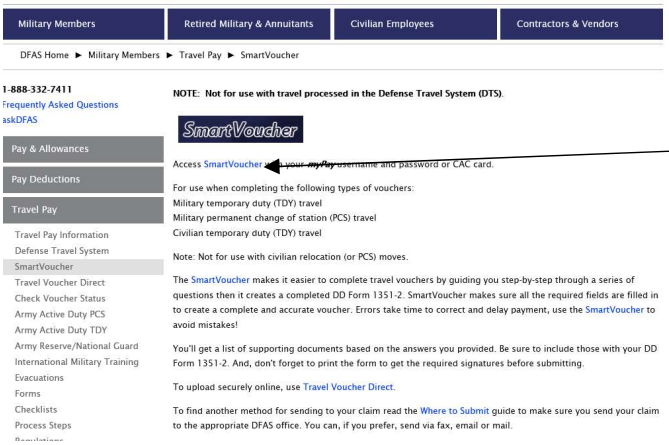
User Signature_____ Date: _____

Permanent Change Of Station (PCS) Voucher Submission

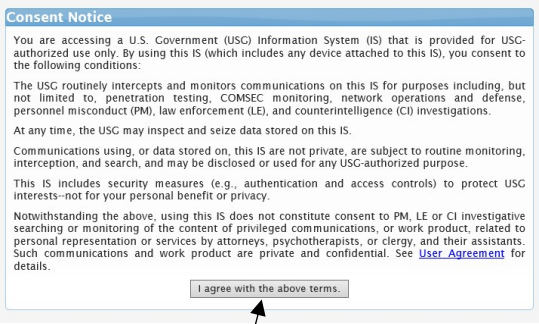
https://www.dfas.mil/militarymembers/travelpay/forms.html



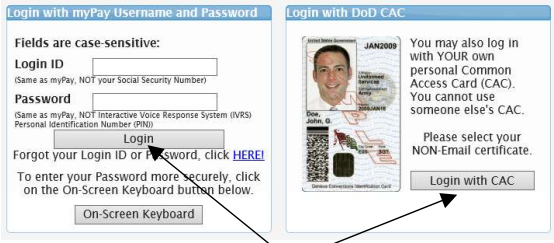
Proceed to web site and select SmartVoucher Hyper link.



Read all instructions the select Hyper link to cont.



Select "I Agree".



Login

Create New VCHR then follow instructions.

DEPARTMENT OF THE NAVY
CHIEF OF NAVAL AIR TRAINING
250 LEXINGTON BLVD SUITE 102
CORPUS CHRISTI TX 78419-5041

CHIEF OF NAVAL AIR TRAINING
EQUAL OPPORTUNITY AND EQUAL EMPLOYMENT OPPORTUNITY POLICY

1. The United States Navy is dependent upon the unique abilities, talents and capabilities of each and every Sailor, Marine, civilian federal employee and contractor. The Naval Air Training Command (NATRACOM) is a high-performance organization that relies on its dynamic and diverse workforce to accomplish critical national security missions.

2. Acts of unlawful discrimination and sexual harassment are contrary to our Core Values of Honor, Courage and Commitment. Sailors and civilians who model Navy Core Values do not engage in negative behaviors nor condone these actions in others. Additionally, negative practices adversely affect good order and discipline, unit cohesion, mission readiness, and prevent our Navy from attaining the highest level of operational readiness.

3. I am fully committed to equal opportunity. I expect those in positions of authority to ensure that an equal opportunity climate is maintained throughout the command and discrimination complaints are investigated promptly and seriously. No individual shall take reprisal action against a person who provides information on an incident of unlawful discrimination or sexual harassment. I also expect all NATRACOM personnel to treat each other and those we serve with respect and dignity.

4. It is each person's responsibility to promote command morale and quality of service by providing a work environment in which all personnel can perform to their maximum ability, unimpeded by institutional or individual biases based on race, color, national origin, sex, age, religion, or disability. Leaders and supervisors at all levels must create and maintain a positive environment through effective communication, training, education, enforcement, assessment, and personal example.

G. N. HARRIS

DEPARTMENT OF THE NAVY
CHIEF OF NAVAL AIR TRAINING
250 LEXINGTON BLVD SUITE 102
CORPUS CHRISTI TX 78419-5041

CHIEF OF NAVAL AIR TRAINING
SEXUAL HARASSMENT AND ANTI-HARASSMENT POLICY STATEMENT

Ref: (a) SECNAV 5300.26D
(b) OPNAVINST 5354.1F
(c) 29 C.F.R. 1614
(d) 10 U.S.C. 1561

1. The fundamental mission of the Navy is national defense and each member of our team, Sailor and civilian, is a critical part of that effort. Towards that end, we must cultivate a work place where people feel valued and respected, and where every individual can reach their full potential. Harassing behavior is detrimental to our mission and our people, and will not be tolerated at this command nor within the Department of the Navy. Therefore, all hands are reminded that sexual harassment and other forms of unlawful harassment are prohibited under federal law. Generally, unlawful harassment is defined as verbal or physical conduct that denigrates or shows hostility to another because of their sex/gender, sexual orientation, race, color, national origin, age, religion, disability and/or genetic information. Harassing behavior includes, but is not limited to: derogatory/offensive statements, jokes, posters, emails, texts, faxes, unwelcome comments and touching.

2. Per references (a) and (b), individuals who are subject to or observe harassing behavior should immediately report the incident(s) to the appropriate supervisory level if: (1) the behavior does not stop after the harasser has been told the behavior is offensive and unwelcome; (2) the employee is uncomfortable in addressing the harasser; or (3) the behavior is severe or possibly criminal in nature. Individuals who feel they are subjected to sexual harassment or any form of unlawful harassment should feel comfortable reporting the situation immediately without fear of retaliation or reprisal.

3. In addition to using the chain of command, avenues to report and seek redress for unlawful harassment include:

a. Service members may contact the NATRACOM Command Managed Equal Employment Officer (CMEEO) at (361) 961-3666 to discuss:

(1) Use of the Informal Resolution System;

(2) Filing of a formal complaint.

b. Civilian employees may:

(1) Contact the COMPACFLT Southwest EEO In-Take Line at (619) 532-3147 (DSN 552) to report and/or file a discrimination complaint pursuant to references (c) and (d);

(2) Contact the NATRACOM local HR Office at (361) 961-1781 to discuss administrative grievance procedures.

4. All leaders, managers, and supervisors shall adhere to and enforce this policy. Reported incidents of harassment will be thoroughly investigated and dealt with promptly, fairly, and effectively. If the alleged harassment is substantiated, immediate and appropriate action will be taken to remedy the situation. Any service member or civilian who is found to have committed sexual harassment or any other unlawful harassment will be subject to appropriate disciplinary and/or administrative actions.

G. N. Harris

G. N. HARRIS

DEPARTMENT OF THE NAVY
CHIEF OF NAVAL AIR TRAINING
250 LEXINGTON BLVD SUITE 102
CORPUS CHRISTI TX 78419-5041

CHIEF OF NAVAL TRAINING
SAFEGUARDING CONTROLLED UNCLASSIFIED INFORMATION

Ref: (a) DOD M-5200.01, Volume 4
(b) DEPSECDEF Memo of 14 Aug 14

1. It is the policy of the Chief of Naval Air Training (CNATRA) that all authorized Naval Air Training Command (NATRACOM) users of DoD information systems, and those with access to Controlled Unclassified Information, understand and comply with policy and guidance provided in references (a) and (b) to prevent unauthorized disclosures. In addition to classified information, certain types of unclassified information in the custody and control of NATRACOM activities require application of access and distribution controls and protective measures. Controlled Unclassified Information (CUI) is a term that encompasses a wide range of information categories, to include Personally Identifiable Information (PII), law enforcement sensitive information, proprietary commercial or financial information received on a privileged basis, information related to physical security or protected critical infrastructure, export-controlled information, etc. If released, such information may pose a threat to security and to DoD operations and missions. All DoD unclassified information must be properly reviewed and approved for release through normal processes before it is provided to the public, to include via posting to publicly accessible websites.

2. CNATRA Department Heads/Special Assistances and NATRACOM Commands are to familiarize themselves with the types of CUI within their organization, and institute effective safeguards with respect to the handling, storage, and dissemination of such CUI. Where dissemination of CUI is required in the conduct of official DoD business, all personal will ensure that such dissemination is consistent with any and all controls specifically applicable to such information. When transmitting electronically, utilize only approved secure communication systems and/or appropriate protective measures (e.g., encryption). Ensure recipients of CUI are properly informed of the nature of information being transmitted, and any handling requirements and restrictions.

3. Data owners are responsible to ensure that CUI data stored on electronic devices (e.g., File Servers, Shared Drives, and External Storage Devices) are properly protected with encryption and access permissions. Only users with the need to view or access the files should be given permissions. Users who no longer need the access should be removed immediately. In instances of unauthorized disclosures of CUI, notification will be immediately made to the CNATRA Security Manager. Data spillages and unauthorized disclosures must be aggressively monitored, and commanders and supervisors at all levels shall investigate and, when they deem appropriate, take appropriate administrative and/or disciplinary actions with respect to those who are found to have caused or contributed to such incidents. Commanders and supervisors will, as they deem appropriate, suspend user accounts for willful violations or while corrective actions are pending.

4. Training on protection of CUI will be incorporated into NATRACOM indoctrination briefings, as well as annual information assurance briefs. Refresher training may be ordered, as necessary, in response to incidents. Work center supervisors are to ensure that members, employees, and contractors handling CUI are properly trained on specific procedures related to the specific marking, storage, and dissemination controls.

G. N. Harris

G. N. HARRIS

DEPARTMENT OF THE NAVY
CHIEF OF NAVAL AIR TRAINING
250 LEXINGTON BLVD SUITE 102
CORPUS CHRISTI TX 78419-5041

CHIEF OF NAVAL AIR TRAINING
PRIORITY PLACEMENT PROGRAM (PPP) POLICY STATEMENT

Ref: (a) Priority Placement Program Handbook, July 2011

1. It is the Department of Defense (DoD) policy to minimize the adverse effects on employees caused by action, such as reduction-in-force, base closures, realignments, consolidation, contracting out, position classification decisions, rotation from overseas, and transfers of function. Reference (a) is the primary means for implementing this policy and procedures for the operation and administration of the program throughout the DoD.

2. The PPP consists of several subprograms with the primary purpose of placing DoD employees who have been adversely affected through no fault of their own. Managers can expect that vacancies will only be matched with PPP registrants who are well qualified and that any registrant matched against a vacancy will have satisfactory performance and conduct.

3. As the DoD continues transforming the military to meet the challenges of the 21st century, the civilian workforce will experience the evolutionary effect of base realignment and closure, global rebasing, and force modernization. Based on past performance, DoD can expect PPP to play a vital role in minimizing the disruption that inevitably accompanies such significant change.

4. It is my expectation that all managers, supervisors and staff officials comply with the policies and procedures of the PPP, including the following:

a. Registrants placed through the PPP will be treated equitably and fairly.

b. Placement assistance efforts must be adequately supported. This includes making available the necessary personnel and funds to support an effective program.

c. Grade and/or pay retention (if applicable) must be provided to otherwise eligible employees placed through the PPP.

CHIEF OF NAVAL AIR TRAINING
PRIORITY PLACEMENT PROGRAM (PPP) POLICY STATEMENT

5. The success of the PPP depends largely on the cooperation of supervisors, managers and affirmative command-level support. Therefore, with this statement, I affirm my personal commitment to support the PPP.

G. N. Harris

G. N. HARRIS

DEPARTMENT OF THE NAVY
CHIEF OF NAVAL AIR TRAINING
250 LEXINGTON BLVD SUITE 102
CORPUS CHRISTI TX 78419-5041

CHIEF OF NAVAL AIR TRAINING
NAVY OCCUPATIONAL SAFETY AND HEALTH POLICY STATEMENT

Navy Safety Programs exist to enhance operational readiness by preserving human life and material resources. For these programs to succeed strict adherence to standard operating procedures, established maintenance practices, Navy Occupational Safety and Health (NAVOSH) standards, and Navy directives are required.

I want to impress upon each member of the CNATRA Team, which includes military, government civilian employees, and contractor personnel, my total commitment to all of our Command's Safety Programs. We will never sacrifice safety for production. Our goal is to accomplish each task professionally, with zero injuries, incidents, or mishaps.

CNATRA's formal Safety Program is built on the foundation of the seven Principles of Operational Excellence:

Integrity
Do the right thing. Adhere to the highest standards at all times.

Level of Knowledge
Know your job and procedures. Never stop learning.

Procedural Compliance
By the book procedures. No short cuts. Fight complacency.

Formal Communication
Use clearly stated and standardized language that minimizes misunderstanding.

Questioning Attitude
Speak up, ask and act when you know something is not right.

Forceful Backup
Speak up, ask and act when you know something is wrong.

Risk Management
Identify, understand and mitigate risk.

The Principles of Operational Excellence shall be used in all levels of planning and apply to every activity at all times. Following and adhering to these principles will ensure safe

mission or activity execution, no matter your role or experience. The most important link in the Safety Chain remains you, the individual member. I task each of you to identify potential hazards and eliminate them before they create accidents. In no case should anyone fear reprisal or second-guessing when acting in the interest of safety.

I will ensure that CNATRA provides a safe work environment and that all resources meet or exceed requirements for safety and health. The Safety Department will constantly educate, train, and monitor the overall Safety Program for full compliance. Each of us must do our part by conducting ourselves in a professional manner.

G. N. Harris

G. N. HARRIS

DEPARTMENT OF THE NAVY
CHIEF OF NAVAL AIR TRAINING
250 LEXINGTON BLVD SUITE 102
CORPUS CHRISTI TX 78419-5041

CHIEF OF NAVAL AIR TRAINING
DRUG AND ALCOHOL POLICY STATEMENT

Ref: (a) OPNAVINST 5350.4D

1. The Naval Air Training Command is a drug-free workplace and use of illegal drugs will not be tolerated. With regard to alcohol, employees should focus on the de-glamorization of alcohol, responsible behavior, and positive after-work activities.

2. Misuse of drugs and alcohol is incompatible with the high standards of conduct and performance expected of the CNATRA team. Management shall pursue every incident of misuse affecting the workplace and take appropriate action including removal from federal service.

3. Military members will be tested randomly for drug or alcohol use. All military members shall ensure that their medical records contain all prescribed medicines. Per reference (a), Commanding Officers may use the Alcohol Detection Device to test military members at their discretion.

4. There are programs available to assist with substance dependence or addiction. Civilian employees are encouraged to seek assistance through the Civilian Employee Assistance Program (CEAP) by contacting the CEAP administrator or by calling 844-366-2327. Military members should contact the Drug and Alcohol Program Advisor (DAPA). If you suspect misuse by a co-worker, please contact the DAPA or CEAP, as appropriate.

5. Again, we will not tolerate the misuse of drugs and/or alcohol as it negatively impacts the people, readiness, and efficiency of the NATRACOM mission.

G. N. HARRIS

DEPARTMENT OF THE NAVY
CHIEF OF NAVAL AIR TRAINING
250 LEXINGTON BLVD SUITE 102
CORPUS CHRISTI TX 78419-5041

CHIEF NAVAL AIR TRAINING SAFETY POLICY STATEMENT

I am committed to ensuring the safety of each member of the CNATRA team, including military, government civilian employees, and contractor personnel. Safety programs protect the people and equipment we need to accomplish our mission. Rather than a barrier to operations, they support our ability to efficiently train aviators by conserving valuable resources. We will never sacrifice safety for production.

CNATRA's safety programs are founded on the **Principles of Operational Excellence:**

Integrity

Do the right thing. Adhere to the highest standards at all times.

Level of Knowledge

Know your job and procedures. Never stop learning.

Procedural Compliance

By the book procedures. No short cuts. Fight complacency.

Formal Communication

Use clearly stated and standardized language that minimizes misunderstanding.

Questioning Attitude

Speak up, ask and investigate when you suspect something is not right.

Forceful Backup

Speak up, ask and act when you know something is wrong.

Risk Management

Identify, understand and mitigate risk.

CHIEF NAVAL AIR TRAINING SAFETY POLICY STATEMENT

Professionalism is the key to successful, mission-focused safety. I expect each member of the CNATRA team to set an example that embodies commitment, courage, and self-discipline.

Everyone must understand and comply with the safety programs that apply to their job. The Navy Occupational Safety and Health (NAVOSH) program, the Aviation Safety program, and the Naval Air Training and Operating Procedures Standardization (NATOPS) program define acceptable practices and safety standards. By the book adherence is expected.

The key to preventing mishaps is you. You are empowered to stop any unsafe act, situation or evolution. Report unsafe conditions so corrections can be made. Our goal is zero mishaps. Our mission depends on safe execution, and our safety programs depend on you!

G. N. Harris

G. N. HARRIS

Service Member's Group Life Insurance (SGLI) Online Enrollment System (SOES)

- Beneficiaries information is not disappearing from
Service member's Group Life Insurance (SGLI) Online Enrollment System (SOES). First time users must enter their beneficiary information. That information was not pre-loaded into SOES.

SOES automatically creates the Sailors record by using the SGLI/FSGLI coverage amount and effective date stored in the Defense Enrollment Eligibility Reporting System. In order for the SOES record to be complete and considered authoritative, Sailors must log into the SOES application to provide beneficiary name(s), share(s) of proceeds, and to certify the record with a digital signature. Sailors who have declined coverage previously and want to continue with no coverage have no required action.

If you are a Service member previously certified in SOES your beneficiary information has not disappeared.

For Service members that have not yet certified in SOES, your current SGLV-8286 form on file in your OMPF will continue to be the authoritative record until the above actions are completed.

Per NAVADMIN 085/17, Service member's shall complete their SOES record by April 2018.

Service members can access SOES by navigating to My Navy Portal at https://my.navy.mil and selecting the milConnect tab. Once logged into milConnect, select the "SOES" option under the "Benefits" tab. Access requires a Common Access Card, DFAS (myPay) account, or DS LOGON account.

For more information, take the online training course available at http://www.benefits.va.gov/INSURANCE/training/SOES/SOES.htm

Thank you,
Navy Personnel Command
PERS-2

Servicemembers' Group Life Insurance
Election and Certificate of Coverage

Name: [redacted]

SSN: [redacted]
Branch of Service: Navy

Your SGLI Coverage Amount as of 10/25/2018: $400,000

Your SGLI Beneficiary Designation as of 10/25/2018

Primary/ Secondary	Name and Address	Social Security Number	Relationship	Share of Proceeds	Payment Option
Primary	[redacted]	XXXX[redacted]	Spouse	100%	Lump Sum
Secondary	[redacted]		Child	Equal Shares	Lump Sum
Secondary	[redacted]		Child	Equal Shares	Lump Sum

Your Family SGLI Spouse Coverage Amount as of 10/25/2018: $0

Your Family SGLI Child Coverage

If you have dependent children, each dependent child is automatically covered for $10,000.

Your Family SGLI Beneficiary

You, the Servicemember, are the beneficiary for spouse and child coverage.

Date Certified: [redacted]

Electronic Signature [redacted]	[redacted]

Servicemembers' Group Life Insurance
Election and Certificate of Coverage

About this Certificate

This Certificate explains in general terms your benefits, as the person insured for Servicemembers' Group Life Insurance (SGLI), under the provisions of a Group Life Insurance Policy (Group Policy) purchased from a commercial life insurance company by the Department of Veterans Affairs (VA) in accordance with the provisions of subchapter III of chapter 19, title 38, United States Code.

The Group Policy that provides the insurance referred to in this Certificate may be modified or terminated as may be required by any change to the law or for other reasons as provided in the Group Policy. Any such modification or termination, however, will not affect any claim arising from death before the effective date of such modification or termination. This Certificate is not a contract of insurance. **Possession of this Certificate does not guarantee coverage at time of claim.** Your benefits under the law and the Group Policy are dependent upon the facts in your individual case.

About SGLI

SGLI is term insurance. It builds no cash, loan, paid up or extended insurance values. You cannot assign it to anyone. The maximum amount of insurance allowed under the provisions of the law is $400,000, but you may decline or elect a lesser amount of coverage in $50,000 increments.

Combined Coverage

You may not carry a combined amount of Servicemembers' Group Life Insurance and Veterans' Group Life Insurance (VGLI) in excess of $400,000. If you have returned to duty and retained Veterans' Group Life Insurance, please notify the Office of Servicemembers' Group Life Insurance immediately. Coverage under the group life insurance policy does not affect your right to retain any other government or private insurance, or your entitlement to other Veterans' benefits.

Beneficiaries

You may name a beneficiary or beneficiaries to receive the proceeds of your SGLI coverage. You do not need the consent of anyone to make or change a beneficiary designation.

If you name more than one primary beneficiary and one or more of them predeceases you, SGLI will pay the shares equally among the remaining primary beneficiaries. If you have no surviving primary beneficiaries, SGLI will pay the insurance benefit to the secondary beneficiaries.

If you do not name a beneficiary, or there are no surviving primary or secondary beneficiaries, or you indicate that payment should be made by law, SGLI will pay the insurance benefit in the following order:

1. Your widow or widower
2. Your children in equal shares (the share of any deceased child will be distributed equally among the descendants of that child)
3. Your parent(s) in equal shares or all to surviving parent
4. A duly appointed executor or administrator of your estate
5. Other next of kin

End of Coverage

If you request to cancel your SGLI coverage, it will end on the last day of the month in which you canceled coverage. If you cancel your coverage and want to restore it, you will have to meet good health requirements.

If you separate from service, your coverage will end 120 days after separation. If you are totally disabled when you separate from service, your coverage will end the earliest of two years following separation or when you cease to be totally disabled, but no less than 120 days from separation.

Coverage will also end if the Group Policy terminates.

Conversion of Insurance

If you have SGLI coverage when you separate from service, you can apply for Veterans' Group Life Insurance. You also have the right to convert your coverage to an individual commercial policy. To convert your coverage, contact the Office of Servicemembers' Group Life Insurance at 1-800-419-1473.

About FSGLI

If you have full-time SGLI coverage, Family Servicemembers' Group Life Insurance (FSGLI) provides coverage to your spouse and unmarried dependent children. If you are married or get married after joining the service, FSGLI automatically covers your spouse, unless your spouse is also a member of the uniformed services and you were married on or after January 2, 2013. You can apply for FSGLI coverage for your military spouse using the SGLI Online Enrollment System at www.ebenefits.va.gov. The maximum amount of spousal coverage is $100,000, but cannot exceed the amount of the member's coverage. Your unmarried dependent children are covered for $10,000 each.

Beneficiary

You, the Servicemember, are always the beneficiary for spouse and child coverage.

End of FSGLI Coverage

FSGLI coverage will end due to any event that causes your full-time SGLI coverage to end, or if your spouse or child becomes ineligible to be covered under FSGLI. You can also choose to cancel FSGLI spouse coverage at any time; however, FSGLI child coverage is not affected by the cancellation of FSGLI spouse coverage. FSGLI child coverage will remain in effect as long as you have full-time SGLI coverage and your dependent child qualifies as an insurable dependent. Spouse coverage remains in effect for 120 days after the event that ended coverage.

Conversion of Insurance

When FSGLI coverage ends, your spouse can convert his or her FSGLI spouse coverage to a commercial life insurance policy. Dependent child coverage cannot be converted. Your spouse can get information about conversion by contacting the Office of Servicemembers' Group Life Insurance at 1-800-419-1473.

Premiums

The premium for your coverage will be deducted from your service pay or otherwise collected from you by the uniformed service.

Claims

Upon death, the Casualty Assistance Office for your branch of service will assist you or your beneficiary in filing a claim for the insurance proceeds. These claims are submitted to the Office of Servicemembers' Group Life Insurance. If you or your beneficiary have any questions about the status of a claim after it has been sent to OSGLI, you or your beneficiary may call 1-800-419-1473 for claim information.

Forfeiture

Any person guilty of mutiny, treason, spying, or desertion, or who, because of conscientious objections, refuses to perform service in the Armed Forces of the United States or refuses to wear the uniform of such force, shall forfeit all rights to the insurance. No insurance shall be payable for death inflicted as a lawful punishment for crimes or for military or naval offense, except when inflicted by an enemy of the United States.

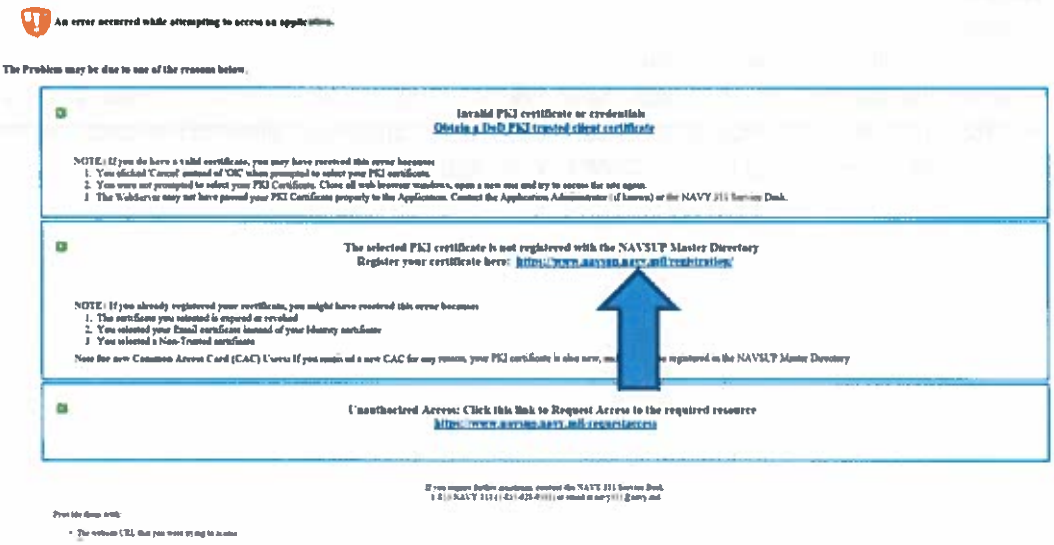
For More Information

For more information on policy provisions, please refer to the SGLI VGLI Handbook at www.insurance.va.gov.

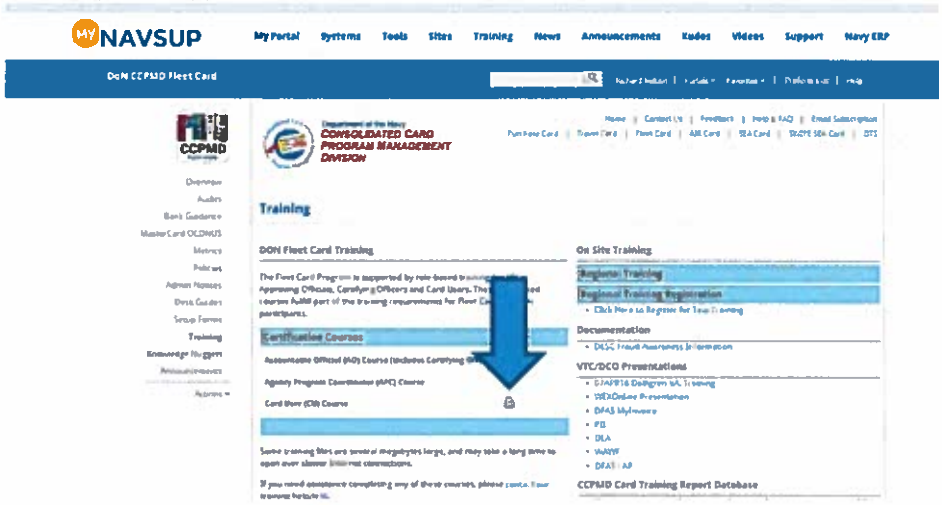
DUTY DRIVER FUEL CARD TRAINING INSTRUCTIONS

*****Wait until you know your .mil email before starting this training*****

1. Type https://www.navsup.navy.mil/public/navsup/ccpmd/ into internet explorer browser
2. Scroll the Bottom of page click **FLEET CARD** (*If it requires you to create an account on NAVSUP continue to step 3 if not proceed with step 8b.)*
3. Fill out the line items appropriately then select I am not a Robot and continue
    a. Name: First name Last name
    b. Navy email: blahblahblah@navy.mil
    c. Organization: USN
4. Select Fleet Card Training and Provide PIN for ID Certification
5. This page will pop up. It is normal. Select second link from the top: https://www.navsup.navy.mil/registration/



    a. Provide PIN again (ID cert)
    b. Press continue
6. Select user type "Military" then continue
7. Fill out only the required fields for all pages, and then press finish.
8. Go back to your second tab, should be labeled **NAVSUP-AccessInfo** https://www.navsup.navy.mil/public/ops$public.access_info?p_resource=CCPMD
    a. Click Fleet Card Training (it should take a while…that is a good sign!)
    b. This page will appear…



    c.
    d. Click on the Printer Icon next to **Card User (CU) Course**
9. Right click Program Overview select open in a new tab
    a. Right click Card User Responsibilities select open in a new tab
    b. Once you have read through both tabs select **Click this link**

10. Copy 11 character code on the second line item (be careful not to copy the extra space after the code)
    a. On line item number 4 select **card user**
11. Paste code into box and continue
12. Fill in appropriate information for registering:
    Enter First Name
    Enter Middle Initial
    Enter Last Name
    Enter PIN (first two letters of your last name + last four of your social security number)
    Enter Users e-mail address; Re-enter Users e-mail address (must be navy email address [.mil])
    Enter Sites APC's Name: Sheri Hoffman
    Enter Your Command Name/CTW-6
    Enter – Level 4/NAVFAC
    Enter – Level 5/Southeast
    Enter – Level 6/UIC 69450
    Drop down Select–Printable PDF as Training Method
13. Once you have completed the training, you will certify having done so by checking the box "I agree to the above statement." Click the "Record Training" button and the certificate will be displayed allowing the card user to print and save. Your certificate will be registered in the CCPMD Training Database

ADMINISTRATIVE REMARKS
NAVPERS 1070/613 (REV. 08-2012) PREVIOUS EDITIONS ARE OBSOLETE SUPPORTING DIRECTIVE MILPERSMAN 1070-320

SHIP OR STATION:

NAS PENSACOLA

SUBJECT:

HIGH RISK ACTIVITIES SAFETY ACKNOWLEDGEMENT

☐ PERMANENT ☒ TEMPORARY

AUTHORITY *(IF PERMANENT)*

Initials

_____ I acknowledge that I have been briefed ion the conduct of High Risk Recreational Activities.

_____ I understand I am required by CNATRAINST 3058.1 to perform an appropiate risk management and receive approval from my Chain of Command prior to participating in any high risk recreational activity. This applies to all times to include off duty, on leave and TAD.

_____ I fully understand that the definition of a high risk recreational activity is any non-mission activity that presents ssignificant risk of serious injury or death and includes but is no limited to:

- Operation of powered/unpowered aircraft for recreational flight (e.g. flying, gliding).
- Operation of powered watercraft (e.g. boating, waterskiing, jet-skiing). Passengers of fishing/pleasure boats are exempted.
- Operation of a motorized vehicle on unprepared terrain at high speeds (e.g. dirt-biking, all-terrain vehicles, snowmobiling).
- Discharge of firearms (e.g. hunting). Target/range shooting in a controlled indoor/outdoor range is exempted.
- Gravity sports involving the use of a parachute, strap or sled to glide or arrest momentum (e.g. parasailing,skydiving, bungee jumping, street luge). Supervised theme park rides are exempted.
- Other activities in which height, depth or speed involved pose a significant risk of injury or death (e.g. scuba diving, rock/ mountain climbing, ski jumping).
- For activities not specifically mentioned, unit Commanding Officers shall determine if the activity is high-risk and falls under the purview of this instruction.

_____ I fully understand that conducting high risk recreational activities is a personal choice and I am personally accountable for my actions. I understand that CNATRAINST 3058.1 is a lawful General Order and violation of it is subject to potential disciplinary action under article 92 of the UCMJ. Additionally, violations of the CNATRAINST 3058.1 may be considered in making line of duty/ misconduct determinations for injuries received ON or OFF base.

Signature/date:_____

ENTERED AND VERIFIED IN ELECTRONIC SERVICE RECORD:

VERIFYING OFFICIAL RANK OR GRADE/TITLE:	DATE:	SIGNATURE OF VERIFYING OFFICIAL:	
NAME (LAST, FIRST, MIDDLE):		SOCIAL SECURITY NUMBER: ON FILE	BRANCH AND CLASS:

ADMINISTRATIVE REMARKS
NAVPERS 1070/613 (REV. 08-2012) PREVIOUS EDITIONS ARE OBSOLETE SUPPORTING DIRECTIVE MILPERSMAN 1070-320

SHIP OR STATION:

NAS PENSACOLA

SUBJECT:	☐ PERMANENT ☒ TEMPORARY
MOTORCYCLE SAFETY ACKNOWLEDGEMENT	AUTHORITY *(IF PERMANENT)*

Initials

_____I acknowledge that I have been briefed on motorcycle safety.
_____I understand that operating a motorcycle is an inherently high-risk activity and as such I will abide by all regulations as outlined in OPNAVINST 5100.12J.
_____I fully understand that operating a motorcycle is a personal choice and I am personally accountable for my actions, such as reckless driving or the absence of PPE. I understand that OPNAVINST 5100.12J is a lawful general order and violations of it are subject to potential disciplinary action under article 92 of the UCMJ. Additionally, violations of OPNAVINST 5100.12J may be considered in making line of duty/misconduct determinations for injuries received on or off base.
_____I possess a valid motorcycle license: yes/no. State____ Expiration_____
_____I understand that possessing a motorcycle license means that I am a motorcycle operator even if I do not actively ride, and will comply with OPNAVINST 5100.12J. I may choose to opt-out of being a motorcycle operator and the training required thereof. In doing so, I relinquish my privileges to operate any motorcycle belonging to myself or anyone else. I may resume riding by refiling this form with a command safety representative and complying with all training requirements.
_____I acknowledge that if I do not currently own a motorcycle, I am required to notify the chain of command if I plan to or do purchase a motorcycle. I am required to notify my Command if I change the type of motorcycle I own.

The following section is for motorcycle operators only

_____I am/am not (circle one) giving up my motorcycle riding privileges until further notice.
_____I own/do not own (circle one) a motorcycle. The primary motorcycle I operate is:
make/model_____ sport bike_____ cruiser/standard_____ cc_____
_____I fully understand that personal protective equipment (PPE) is mandatory per OPNAVINST 5100.12J and must be worn while operating or riding on a motorcycle regardless of location or duty status. Mandatory PPE requirements are: a properly fastened protective helmet that meets U.S. Dept. of Transportation (DOT) standards; protective eye devices designed for motorcycle operators (impact or shatter resistant safety glasses, goggles, wrap around glasses or face shield properly attached to the helmet); sturdy over the ankle footwear; long-sleeved shirt or jacket, long-legged trousers; full fingered gloves or mittens designed for use on a motorcycle. The following PPE is recommended for use: reflective outer garments or vest at night; brightly colored outer garments during the day; garments constructed of abrasion resistant materials such as leather, Kevlar, and/or Cordura; garments containing impact absorbing padding.
_____I understand that I am required by OPNAVINST 5100.12J to attend level I (e.g. Motorcycle Safety Foundation Basic Rider Course or State-approved course) and level II motorcycle training at no cost. Non-sport bike rider level II courses include the MSF experienced rider course/BRC II and advanced rider course. Level II courses for sport bike riders include the advanced rider course or military sportbike rider course. Level II training shall be completed within 60 days of level I training or upon changing type of motorcycle ridden. Refresher training is required every three years.
_____I understand I am required to turn in a copy of my current motorcycle registration, insurance, base decal number, and documentation of completion of approved motorcycle training to my chain of command.

Signature/date:_____

ENTERED AND VERIFIED IN ELECTRONIC SERVICE RECORD:

VERIFYING OFFICIAL RANK OR GRADE/TITLE:	DATE:	SIGNATURE OF VERIFYING OFFICIAL:

NAME (LAST, FIRST, MIDDLE):	SOCIAL SECURITY NUMBER:	BRANCH AND CLASS:
	ON FILE	

Aviation Into-Plane Reimbursement (AIR) Card Program
Card User Statement of Understanding (SOU)

-I certify that I have read the "AIR Card User Guidance." I understand that I am authorized to use the AIR card only for those necessary and reasonable expenses incurred by me for official government business for aviation fuel and related ground services and supplies for DON owned/leased aircraft.

-I certify that I have completed the Card User Certification Course available at https://www.navsup.navy.mil/ccpmd/air_card/training

-I understand that the issuance of this AIR card to me is an extension of the employee-employer relationship and that I am being specifically directed to:

____ Abide by all rules and regulations with respect to the charge card.

____ Use the charge card only for official government business.

____ Notify the APC of any problems with respect to my usage of the charge card.

____ Notify the APC immediately if my charge card is lost or stolen.

(AIR card users must initial all the above provisions.)

-I also understand that failure on my part to abide by these rules or to otherwise misuse the card may result in disciplinary action being taken against me and the loss of my security clearance. I also acknowledge the right of the AIR card APC to revoke or suspend my AIR card privileges if I fail to abide by the terms of this agreement.

-As indicated in the DoD FMR Volume 5, Chapter 33, I am considered an accountable official and as such, I may be held liable to the government for improper use of the AIR card.

_____	_____
(Card User's Signature)	(APC Signature)
_____	_____
(Card User's Printed Name)	(APC Printed Name)
_____	_____
(Card User's Grade/Title)	(APC Series/Grade/Title)