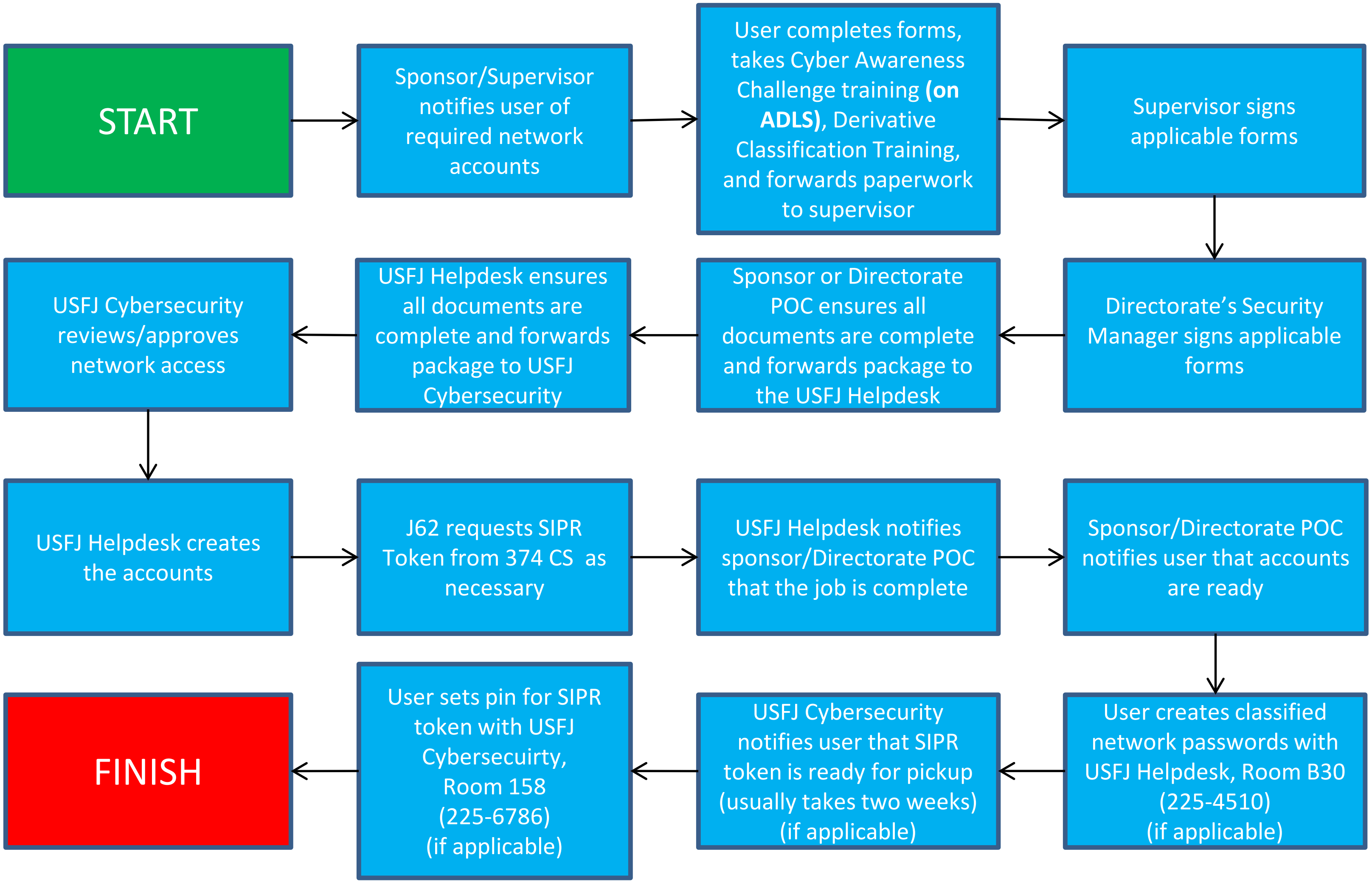
USFJ Network Account Request Overview

- Please review this presentation to ensure that you are filling out the proper paperwork for network access. Be sure to contact your sponsor/supervisor to find out which accounts are required for your position.
- The slides contain each form that will be needed for that specific account type.
- Once you've filled out and compiled all the necessary documents (with supervisor signature) forward them to your directorate's security manager
- Once the directorate security manager fills out their portion, the documents will need to be forwarded to the sponsor or directorate POC for review and processing (this step may not be necessary if your security manager is also your directorate POC)
- If you have any questions during any part of this process, please contact your sponsor or directorate POC.
- For NIPRnet users, an ADLS version of the *Cyber Awareness Challenge* **must** be completed for access to an Air Force network.

USFJ Network Account Request Flowchart



START

Sponsor/Supervisor notifies user of required network accounts

User completes forms, takes Cyber Awareness Challenge training **(on ADLS)**, Derivative Classification Training, and forwards paperwork to supervisor

Supervisor signs applicable forms

Directorate's Security Manager signs applicable forms

Sponsor or Directorate POC ensures all documents are complete and forwards package to the USFJ Helpdesk

USFJ Helpdesk ensures all documents are complete and forwards package to USFJ Cybersecurity

USFJ Cybersecurity reviews/approves network access

USFJ Helpdesk creates the accounts

J62 requests SIPR Token from 374 CS as necessary

USFJ Helpdesk notifies sponsor/Directorate POC that the job is complete

Sponsor/Directorate POC notifies user that accounts are ready

User creates classified network passwords with USFJ Helpdesk, Room B30 (225-4510) (if applicable)

USFJ Cybersecurity notifies user that SIPR token is ready for pickup (usually takes two weeks) (if applicable)

User sets pin for SIPR token with USFJ Cybersecuirty, Room 158 (225-6786) (if applicable)

FINISH

*** IF AT ANYTIME YOU HAVE A QUESTION, CONTACT YOUR SPONSOR/DIRECTORATE POC***

Directorate Info-System Coordinators (ISC) and Security Managers (SM)

J0:		
TSgt Clifford Jackson (ISC & SM)	225-4288	Clifford.j.jackson6.mil@mail.mil
J1:		
SMSgt Katrina McNutt (ISC)	225-4160	katrina.l.mcnutt.mil@mail.mil
J2:		
ISC Ken Eygnor (ISC & SM)	225-9140	ken.w.eygnor.mil@mail.mil
J3:		
SSgt Potter, Kyle A (ISC)	225-4225	kyle.a.potter2.mil@mail.mil
J4:		
SSgt Clariza Johnson (ISC & SM)	225-4705	clariza.c.johnson.mil@mail.mil
Sgt Victor Corena (ISC)	225-4705	victor.j.corena.mil@mail.mil
J5:		
TSgt Darlene McKerracher (ISC & SM)	225-4474	Darlene.r.mckerracher.mil@mail.mil
J6:		
USFJ Networks Helpdesk (ISC)	225-4510	pacom.yokota.usfj.mbx.helpdesk@mail.mil

NOTE: Current 1 Dec 18. Please contact USFJ Help Desk, or IA (225-6771) for more info.

* TIPS *

Cyber Awareness Challenge Training: AFNET NIPR accounts require this training to be completed via ADLS (see next slide for instructions) in order to track training. For TDY personnel, any valid DoD Cyber Awareness Challenge training certificate will be accepted (see http://iatraining.disa.mil/eta/cyberchallenge_v4/launchPage.htm).

Derivative Classification Training: Required for SIPR or CENTRIXS-J accounts. Available at https://securityawareness.usalearning.gov/derivative/index.htm. There is no sign up requirement. All sections must be viewed before the test will load at the end. The certificate may take a while to load, so do not close the browser. If you close the browser, you will have to retake the course. Include the certificate as part of the account request.

DD2875:

- User fills out "Type of Request" through block 12
- Supervisor fills out blocks 13 – 20b
- Directorate Security Manager fills out blocks 28 – 32

AF FORM 4394:

- User fills out blocks 1-4 after reading agreement

SAAR-N:

- *A SAAR-N needs to be filled out for each network the user is requesting access to*
- User fills out "Type of Request" through block 10, then blocks 23 – 25
- Supervisor fills out blocks 11 – 16b
- Block 12 will be "authorized" for a user account or "privileged" for an admin account
- Directorate Security Manager fills out blocks 26 – 30

DD2842:

- User fills out 1a – 1i
- Block 1e, input using the format: first.lastname@usfj.smil.mil

CONTACT INFO:

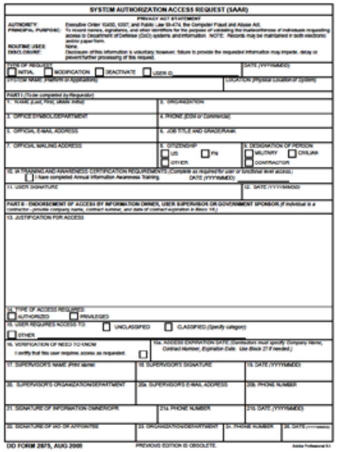
- USFJ Helpdesk: email pacom.yokota.usfj.mbx.helpdesk@mail.mil; DSN 225-6786

FILL OUT EVERY REQUIRED BLOCK LISTED OR IT MAY BE REJECTED AND SLOW DOWN THE ACCOUNT CREATION PROCESS!

AFNET NIPR Account

** Double click form to fill it out**

** Cyber Awareness Challenge* ***MUST*** *be completed on ADLS website. See instructions Below**



SYSTEM AUTHORIZATION ACCESS REQUEST (SAAR)

PRIVACY ACT STATEMENT

DD FORM 2875, AUG 2009 PREVIOUS EDITION IS OBSOLETE.

DD 2875

AF Form 4394

AIR EDUCATION AND TRAINING COMMAND

UNITED STATES AIR FORCE

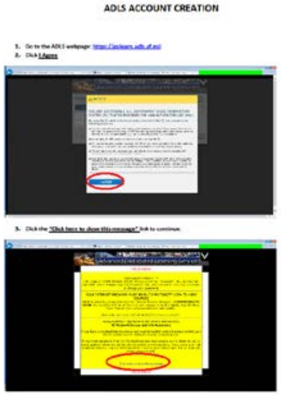
This is to certify that

has successfully completed

conducted this day of in the year of 2018

Cyber Challenge Awareness Training Certificate

SIGNED BY USER



ADLS ACCOUNT CREATION

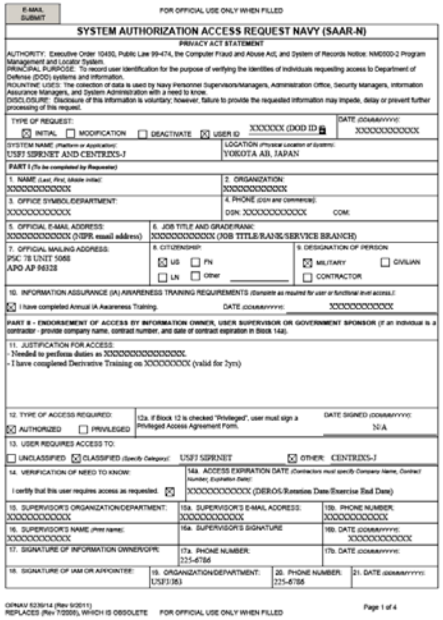
1. Go to the ADLS webpage: https://golearn.adls.af.mil
2. Click I Agree

3. Click the "Click here to show this message" link to continue.

ADLS Instructions

Combined Form for USFJ SIPR & CENTRIXS-JPN Accounts

** Double click form to fill it out**



E-MAIL SUBMIT

FOR OFFICIAL USE ONLY WHEN FILLED

SYSTEM AUTHORIZATION ACCESS REQUEST NAVY (SAAR-N)

PRIVACY ACT STATEMENT

AUTHORITY: Executive Order 10450, Public Law 99-474, the Computer Fraud and Abuse Act, and System of Records Notice: NM05000-2 Program Management and Locator System.
PRINCIPAL PURPOSE: To record user identification for the purpose of verifying the identities of individuals requesting access to Department of Defense (DOD) systems and information.
ROUNTINE USES: The collection of data is used by Navy Personnel Supervisors/Managers, Administration Office, Security Managers, Information Assurance Managers, and System Administration with a need to know.
DISCLOSURE: Disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay or prevent further processing of this request.

TYPE OF REQUEST: ☒ INITIAL ☐ MODIFICATION ☐ DEACTIVATE ☒ USER ID XXXXXX (DOD ID#)
DATE (DD/MMM/YYYY): XXXXXXXXXXX

SYSTEM NAME (Platform or Application): USFJ SIPRNET AND CENTRIXS-J
LOCATION (Physical Location of System): YOKOTA AB, JAPAN

PART I (To be completed by Requester)

1. NAME (Last, First, Middle Initial): XXXXXXXXXXX
2. ORGANIZATION: XXXXXXXXXXX
3. OFFICE SYMBOL/DEPARTMENT: XXXXXXXXXXX
4. PHONE (DSN and Commercial): DSN: XXXXXXXXXXX COM:
5. OFFICIAL E-MAIL ADDRESS: XXXXXXXXXXX (NIPR email address)
6. JOB TITLE AND GRADE/RANK: XXXXXXXXXXX (JOB TITLE/RANK/SERVICE BRANCH)
7. OFFICIAL MAILING ADDRESS:
PSC 78 UNIT 5068
APO AP 96328
8. CITIZENSHIP: ☒ US ☐ FN ☐ LN ☐ Other ____________
9. DESIGNATION OF PERSON: ☒ MILITARY ☐ CIVILIAN ☐ CONTRACTOR
10. INFORMATION ASSURANCE (IA) AWARENESS TRAINING REQUIREMENTS (Complete as required for user or functional level access.)
☒ I have completed Annual IA Awareness Training. DATE (DD/MMM/YYYY): XXXXXXXXXXX

PART II - ENDORSEMENT OF ACCESS BY INFORMATION OWNER, USER SUPERVISOR OR GOVERNMENT SPONSOR (If an individual is a contractor - provide company name, contract number, and date of contract expiration in Block 14a).

11. JUSTIFICATION FOR ACCESS:
- Needed to perform duties as XXXXXXXXXXXXXX.
- I have completed Derivative Training on XXXXXXXX (valid for 2yrs)

12. TYPE OF ACCESS REQUIRED: ☒ AUTHORIZED ☐ PRIVILEGED
12a. If Block 12 is checked "Privileged", user must sign a Privileged Access Agreement Form.
DATE SIGNED (DD/MMM/YYYY): N/A

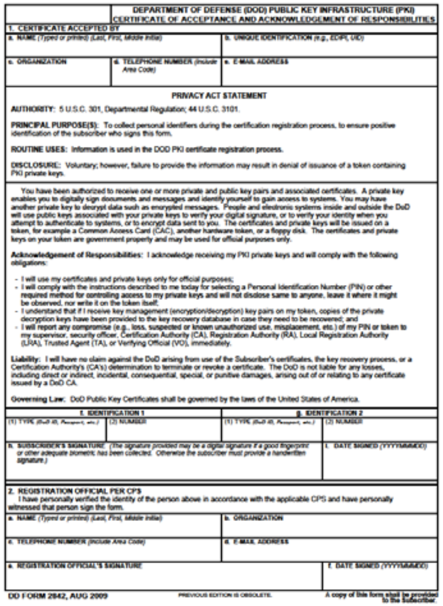
13. USER REQUIRES ACCESS TO: ☐ UNCLASSIFIED ☒ CLASSIFIED (Specify Category): USFJ SIPRNET ☒ OTHER: CENTRIXS-J

14. VERIFICATION OF NEED TO KNOW:
I certify that this user requires access as requested. ☒
14a. ACCESS EXPIRATION DATE (Contractors must specify Company Name, Contract Number, Expiration Date): XXXXXXXXXXX (DEROS/Rotation Date/Exercise End Date)

15. SUPERVISOR'S ORGANIZATION/DEPARTMENT: XXXXXXXXXXX
15a. SUPERVISOR'S E-MAIL ADDRESS: XXXXXXXXXXX
15b. PHONE NUMBER: XXXXXXXXXXX
16. SUPERVISOR'S NAME (Print Name): XXXXXXXXXXX
16a. SUPERVISOR'S SIGNATURE
16b. DATE (DD/MMM/YYYY): XXXXXXXXXXX
17. SIGNATURE OF INFORMATION OWNER/OPR:
17a. PHONE NUMBER: 225-6786
17b. DATE (DD/MMM/YYYY):
18. SIGNATURE OF IAM OR APPOINTEE:
19. ORGANIZATION/DEPARTMENT: USFJ/J63
20. PHONE NUMBER: 225-6786
21. DATE (DD/MMM/YYYY):

OPNAV 5239/14 (Rev 9/2011)
REPLACES (Rev 7/2008), WHICH IS OBSOLETE FOR OFFICIAL USE ONLY WHEN FILLED
Page 1 of 4

Combined SAAR-N SIPR/CENTRIXS-JPN



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

1. CERTIFICATE ACCEPTED BY
a. NAME (Typed or printed) (Last, First, Middle Initial)
b. UNIQUE IDENTIFICATION (e.g., EDIPI, UID)
c. ORGANIZATION
d. TELEPHONE NUMBER (Include Area Code)
e. E-MAIL ADDRESS

PRIVACY ACT STATEMENT

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

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

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

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

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

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

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

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

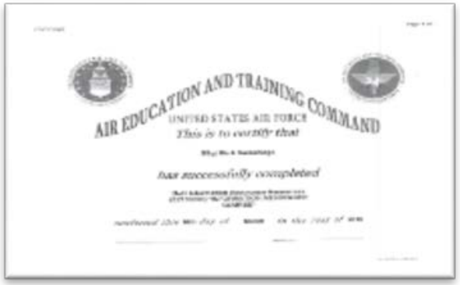
Governing Law: DoD Public Key Certificates shall be governed by the laws of the United States of America.

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

2. REGISTRATION OFFICIAL PER CPS
I have personally verified the identity of the person above in accordance with the applicable CPS and have personally witnessed that person sign the form.
a. NAME (Typed or printed) (Last, First, Middle Initial)
b. ORGANIZATION
c. TELEPHONE NUMBER (Include Area Code)
d. E-MAIL ADDRESS
e. REGISTRATION OFFICIAL'S SIGNATURE
f. DATE SIGNED (YYYYMMDD)

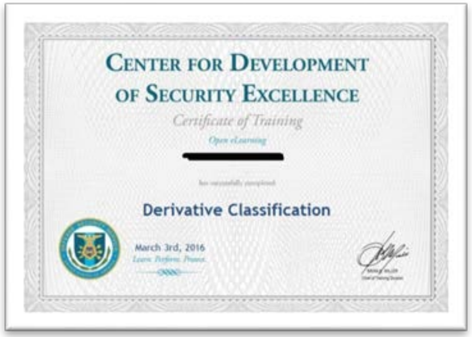
DD FORM 2842, AUG 2009 PREVIOUS EDITION IS OBSOLETE. A copy of this form shall be provided to the Subscriber.

DD Form 2842



AIR EDUCATION AND TRAINING COMMAND
UNITED STATES AIR FORCE
This is to certify that
[illegible]
has successfully completed
[illegible]
conducted this [illegible] day of [illegible] in the year of [illegible]

Cyber Challenge Awareness Training Certificate
SIGNED BY USER

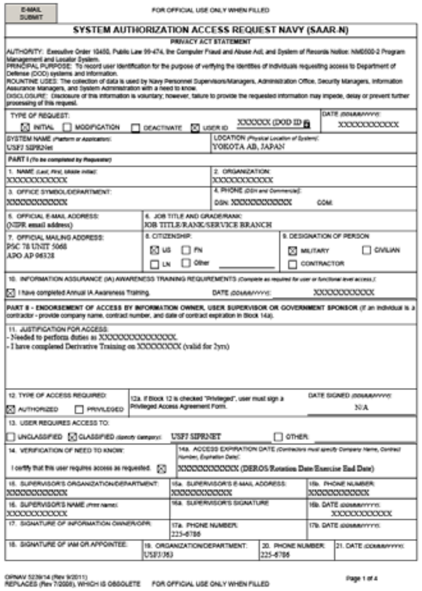


CENTER FOR DEVELOPMENT OF SECURITY EXCELLENCE
Certificate of Training
Open eLearning
[redacted]
has successfully completed
Derivative Classification
March 3rd, 2016
Learn. Perform. Protect.

Derivative Classification Training Certificate
SIGNED BY USER

USFJ SIPR-Only Account Request

** Double click form to fill it out**



E-MAIL SUBMIT

FOR OFFICIAL USE ONLY WHEN FILLED

SYSTEM AUTHORIZATION ACCESS REQUEST NAVY (SAAR-N)

PRIVACY ACT STATEMENT

AUTHORITY: Executive Order 10450, Public Law 99-474, the Computer Fraud and Abuse Act, and System of Records Notice: NM05000-2 Program Management and Locator System.
PRINCIPAL PURPOSE: To record user identification for the purpose of verifying the identities of individuals requesting access to Department of Defense (DOD) systems and information.
ROUNTINE USES: The collection of data is used by Navy Personnel Supervisors/Managers, Administration Office, Security Managers, Information Assurance Managers, and System Administration with a need to know.
DISCLOSURE: Disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay or prevent further processing of this request.

TYPE OF REQUEST: ☒ INITIAL ☐ MODIFICATION ☐ DEACTIVATE ☒ USER ID XXXXXX (DOD ID#)	DATE *(DD/MMM/YYYY)*: XXXXXXXXXXX
SYSTEM NAME *(Platform or Application)*: USFJ SIPRNet	LOCATION *(Physical Location of System)*: YOKOTA AB, JAPAN

PART I *(To be completed by Requester)*

1. NAME *(Last, First, Middle Initial)*: XXXXXXXXXXX	2. ORGANIZATION: XXXXXXXXXXX	
3. OFFICE SYMBOL/DEPARTMENT: XXXXXXXXXXX	4. PHONE *(DSN and Commercial)*: DSN: XXXXXXXXXXX COM:	
5. OFFICIAL E-MAIL ADDRESS: (NIPR email address)	6. JOB TITLE AND GRADE/RANK: JOB TITLE/RANK/SERVICE BRANCH	
7. OFFICIAL MAILING ADDRESS: PSC 78 UNIT 5068 APO AP 96328	8. CITIZENSHIP: ☒ US ☐ FN ☐ LN ☐ Other ____	9. DESIGNATION OF PERSON ☒ MILITARY ☐ CIVILIAN ☐ CONTRACTOR

10. INFORMATION ASSURANCE (IA) AWARENESS TRAINING REQUIREMENTS *(Complete as required for user or functional level access.)*:
☒ I have completed Annual IA Awareness Training. DATE *(DD/MMM/YYYY)*: XXXXXXXXXXX

PART II - ENDORSEMENT OF ACCESS BY INFORMATION OWNER, USER SUPERVISOR OR GOVERNMENT SPONSOR (If an individual is a contractor - provide company name, contract number, and date of contract expiration in Block 14a).

11. JUSTIFICATION FOR ACCESS:
- Needed to perform duties as XXXXXXXXXXXXXX.
- I have completed Derivative Training on XXXXXXXX (valid for 2yrs)

12. TYPE OF ACCESS REQUIRED: ☒ AUTHORIZED ☐ PRIVILEGED	12a. If Block 12 is checked "Privileged", user must sign a Privileged Access Agreement Form.	DATE SIGNED *(DD/MMM/YYYY)*: N/A

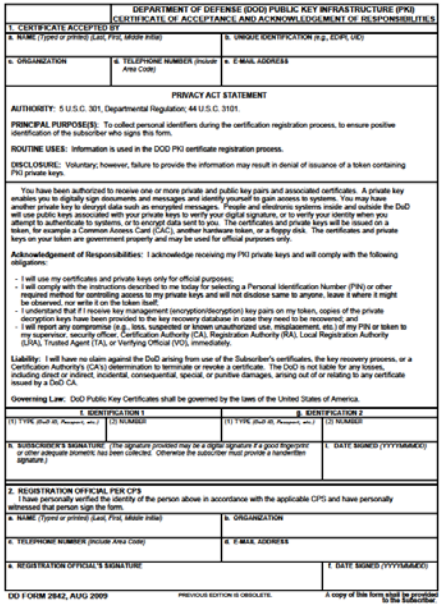
13. USER REQUIRES ACCESS TO:
☐ UNCLASSIFIED ☒ CLASSIFIED *(specify category)*: USFJ SIPRNET ☐ OTHER:

14. VERIFICATION OF NEED TO KNOW: I certify that this user requires access as requested. ☒	14a. ACCESS EXPIRATION DATE *(Contractors must specify Company Name, Contract Number, Expiration Date)*: XXXXXXXXXXX (DEROS/Rotation Date/Exercise End Date)

15. SUPERVISOR'S ORGANIZATION/DEPARTMENT: XXXXXXXXXXX	15a. SUPERVISOR'S E-MAIL ADDRESS: XXXXXXXXXXX	15b. PHONE NUMBER: XXXXXXXXXXX	
16. SUPERVISOR'S NAME *(Print Name)*: XXXXXXXXXXX	16a. SUPERVISOR'S SIGNATURE	16b. DATE *(DD/MMM/YYYY)*: XXXXXXXXXXX	
17. SIGNATURE OF INFORMATION OWNER/OPR:	17a. PHONE NUMBER: 225-6788	17b. DATE *(DD/MMM/YYYY)*:	
18. SIGNATURE OF IAM OR APPOINTEE:	19. ORGANIZATION/DEPARTMENT: USFJ/J63	20. PHONE NUMBER: 225-6788	21. DATE *(DD/MMM/YYYY)*:

OPNAV 5239/14 (Rev 9/2011)
REPLACES (Rev 7/2008), WHICH IS OBSOLETE FOR OFFICIAL USE ONLY WHEN FILLED Page 1 of 4

SAAR-N - SIPR



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

1. CERTIFICATE ACCEPTED BY		
a. NAME *(Typed or printed) (Last, First, Middle Initial)*		**b. UNIQUE IDENTIFICATION** *(e.g., EDIPI, UID)*
c. ORGANIZATION	**d. TELEPHONE NUMBER** *(Include Area Code)*	**e. E-MAIL ADDRESS**

PRIVACY ACT STATEMENT

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

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

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

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

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

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

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

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

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

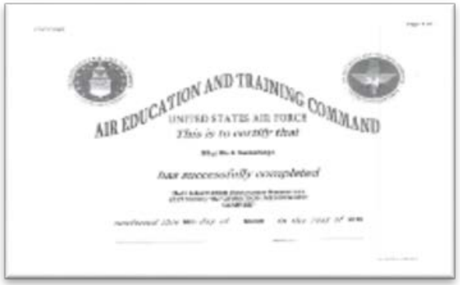
f. IDENTIFICATION 1		**g. IDENTIFICATION 2**	
(1) TYPE *(DoD ID, Passport, etc.)*	(2) NUMBER	(1) TYPE *(DoD ID, Passport, etc.)*	(2) NUMBER
h. SUBSCRIBER'S SIGNATURE *(The signature provided may be a digital signature if a good fingerprint or other adequate biometric has been collected. Otherwise the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

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

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

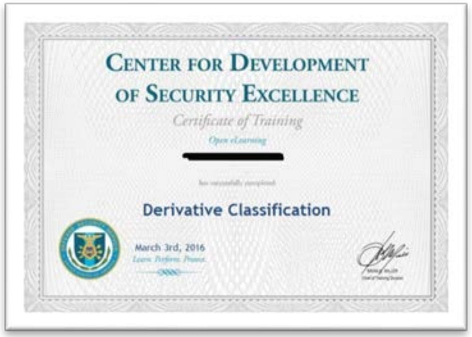
DD FORM 2842, AUG 2009 PREVIOUS EDITION IS OBSOLETE. **A copy of this form shall be provided to the Subscriber.**

DD Form 2842



AIR EDUCATION AND TRAINING COMMAND
UNITED STATES AIR FORCE
This is to certify that
[illegible]
has successfully completed
[illegible]
conferred this [illegible] *day of* [illegible] *in the year of* [illegible]

Cyber Challenge Awareness Training Certificate
SIGNED BY USER

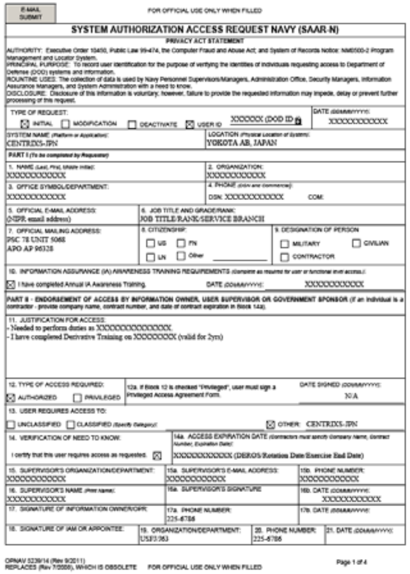


CENTER FOR DEVELOPMENT OF SECURITY EXCELLENCE
Certificate of Training
Open eLearning
[redacted]
has successfully completed
Derivative Classification
March 3rd, 2016
Learn. Perform. Protect.

Derivative Classification Training Certificate
SIGNED BY USER

USFJ CENTRIXS-JPN-Only Account Request

** Double click form to fill it out**



E-MAIL SUBMIT

FOR OFFICIAL USE ONLY WHEN FILLED

SYSTEM AUTHORIZATION ACCESS REQUEST NAVY (SAAR-N)

PRIVACY ACT STATEMENT

AUTHORITY: Executive Order 10450, Public Law 99-474, the Computer Fraud and Abuse Act; and System of Records Notice: NM05000-2 Program Management and Locator System.
PRINCIPAL PURPOSE: To record user identification for the purpose of verifying the identities of individuals requesting access to Department of Defense (DOD) systems and information.
ROUNTINE USES: The collection of data is used by Navy Personnel Supervisors/Managers, Administration Office, Security Managers, Information Assurance Managers, and System Administration with a need to know.
DISCLOSURE: Disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay or prevent further processing of this request.

TYPE OF REQUEST: ☒ INITIAL ☐ MODIFICATION ☐ DEACTIVATE ☒ USER ID XXXXXX (DOD ID#)

DATE *(DD/MMM/YYYY)*: XXXXXXXXXXX

SYSTEM NAME *(Platform or Application)*: CENTRIXS-JPN

LOCATION *(Physical Location of System)*: YOKOTA AB, JAPAN

PART I *(To be completed by Requester)*

1. NAME *(Last, First, Middle Initial)*: XXXXXXXXXXX

2. ORGANIZATION: XXXXXXXXXXX

3. OFFICE SYMBOL/DEPARTMENT: XXXXXXXXXXX

4. PHONE *(DSN and Commercial)*: DSN: XXXXXXXXXXX COM:

5. OFFICIAL E-MAIL ADDRESS: (NIPR email address)

6. JOB TITLE AND GRADE/RANK: JOB TITLE/RANK/SERVICE BRANCH

7. OFFICIAL MAILING ADDRESS:
PSC 78 UNIT 5068
APO AP 96328

8. CITIZENSHIP: ☐ US ☐ FN ☐ LN ☐ Other ______

9. DESIGNATION OF PERSON: ☐ MILITARY ☐ CIVILIAN ☐ CONTRACTOR

10. INFORMATION ASSURANCE (IA) AWARENESS TRAINING REQUIREMENTS *(Complete as required for user or functional level access.)*:
☒ I have completed Annual IA Awareness Training. DATE *(DD/MMM/YYYY)*: XXXXXXXXXXX

PART II - ENDORSEMENT OF ACCESS BY INFORMATION OWNER, USER SUPERVISOR OR GOVERNMENT SPONSOR (If an individual is a contractor - provide company name, contract number, and date of contract expiration in Block 14a).

11. JUSTIFICATION FOR ACCESS:
- Needed to perform duties as XXXXXXXXXXXXXX.
- I have completed Derivative Training on XXXXXXXX (valid for 2yrs)

12. TYPE OF ACCESS REQUIRED: ☒ AUTHORIZED ☐ PRIVILEGED

12a. If Block 12 is checked "Privileged", user must sign a Privileged Access Agreement Form. DATE SIGNED *(DD/MMM/YYYY)*: N/A

13. USER REQUIRES ACCESS TO: ☐ UNCLASSIFIED ☐ CLASSIFIED *(Specify Category)*: ______ ☒ OTHER: CENTRIXS-JPN

14. VERIFICATION OF NEED TO KNOW:
I certify that this user requires access as requested. ☒

14a. ACCESS EXPIRATION DATE *(Contractors must specify Company Name, Contract Number, Expiration Date)*: XXXXXXXXXXX (DEROS/Rotation Date/Exercise End Date)

15. SUPERVISOR'S ORGANIZATION/DEPARTMENT: XXXXXXXXXXX

15a. SUPERVISOR'S E-MAIL ADDRESS: XXXXXXXXXXX

15b. PHONE NUMBER: XXXXXXXXXXX

16. SUPERVISOR'S NAME *(Print Name)*: XXXXXXXXXXX

16a. SUPERVISOR'S SIGNATURE

16b. DATE *(DD/MMM/YYYY)*: XXXXXXXXXXX

17. SIGNATURE OF INFORMATION OWNER/OPR:

17a. PHONE NUMBER: 225-6786

17b. DATE *(DD/MMM/YYYY)*:

18. SIGNATURE OF IAM OR APPOINTEE:

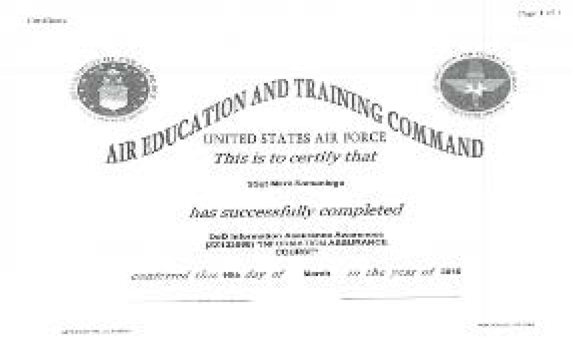
19. ORGANIZATION/DEPARTMENT: USFJ/J63

20. PHONE NUMBER: 225-6786

21. DATE *(DD/MMM/YYYY)*:

OPNAV 5239/14 (Rev 9/2011)
REPLACES (Rev 7/2008), WHICH IS OBSOLETE FOR OFFICIAL USE ONLY WHEN FILLED Page 1 of 4

SAAR-N – CENTRIXS-JPN



Certificate Page 1 of 1

AIR EDUCATION AND TRAINING COMMAND

UNITED STATES AIR FORCE

This is to certify that

[illegible]

has successfully completed

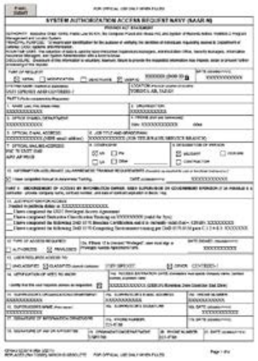
DoD Information Assurance Awareness
[illegible] INFORMATION ASSURANCE
COURSE

conferred this [illegible] *day of* March *in the year of* [illegible]

Cyber Challenge Awareness Training Certificate
SIGNED BY USER

Privileged User (Admin) Account

** Double click form to fill it out**

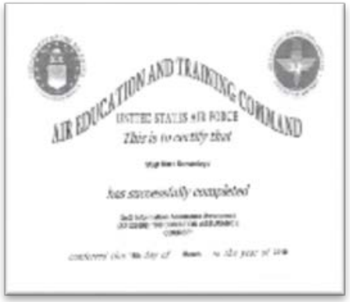


FOR OFFICIAL USE ONLY WHEN FILLED

SYSTEM AUTHORIZATION ACCESS REQUEST NAVY (SAAR-N)

PRIVACY ACT STATEMENT

SAAR-N - Admin
(form can be include multiple
networks as required)



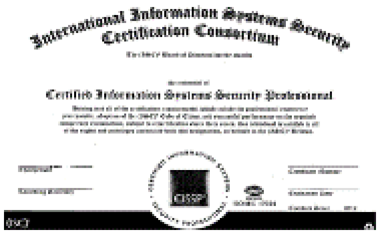
AIR EDUCATION AND TRAINING COMMAND

UNITED STATES AIR FORCE

This is to certify that

has successfully completed

Cyber Awareness Challenge
Training Certificate
SIGNED BY USER

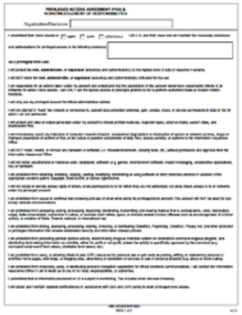


International Information Systems Security Certification Consortium

Certified Information Systems Security Professional

CISSP

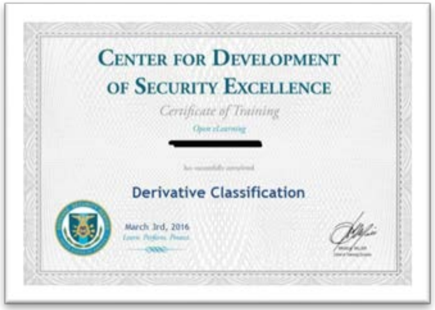
8570 Baseline
Training Certificate
(e.g., Sec+, CISSP)



PRIVILEGED ACCESS AGREEMENT (PAA) &
ACKNOWLEDGEMENT OF RESPONSIBILITIES

Organization/Directorate

Privileged
Agreement Form



CENTER FOR DEVELOPMENT
OF SECURITY EXCELLENCE

Certificate of Training

Open eLearning

[redacted]

has successfully completed

Derivative Classification

March 3rd, 2016

Learn. Perform. Protect.

Derivative Classification
Training Certificate
SIGNED BY USER

Microsoft Certified
Solutions Associate

[redacted]

Has successfully completed the requirements to be recognized as a Microsoft® Certified Solutions Associate: Windows Server 2012.

Date of achievement: [redacted]
Certification number:

Microsoft
CERTIFIED
Solutions Associate

8570 computing environment
training certificate (e.g.,
ACAS, HBSS, MCSA, etc.)
per DoD 8570.01-M para
C3.2.4.8.3

USFJ Temporary NIPR Account Request

- NIPRNet Access
  - If members have an AFNet account:
    - Home station would have to release them prior to arriving at USFJ. USFJ Help Desk would request that the members account be provisioned for use here. This process could take up to 24 hours.
  - If members DO NOT have an AFNet Account:
    - All paperwork required in Slide 5 would need to be accomplished and submitted to the ISC for review. Once ISCs submit paperwork for account creation, at a minimal, it will take 3 business days for the account to be created by Air Force Directory Services.
    - Note: Because this service is not provided by USFJ, it cost USFJ money for each AFNet account created. This account creation should be reserved for mission critical members.

USFJ Temporary SIPR Account Request

- All members on temporary duty to USFJ would need all the required paperwork on slide 6
- All members **will** bring a SIPR Token from their home station.
  - If member does not have a SIPR Token, USFJ can request one be created. This process will take up to 48 hours and should be kept to a minimal due to limited resources.

Note: NO Username/Password will be given out to temporary members.

Other USFJ Temporary Account Request

- For all other account types, see required info on the slide for those.