Print Form

Reset Form

Enter appropriate classification markings

AFADS NETWORK ACCOUNT APPLICATION

A. Applicant Information

First Name: Last Name: Rank/Grade:

Phone Number: Unclas/E-Mail

Organization/Company Name: SSN:

☐ Military ☐ Govt. Civilian ☐ Contractor

I the user certify that:
(1) The computer account will be used in support of an official DoD project/contract.
(2) I will not willfully compromise the account password. (examples of willful compromise include storing the account password in a PC or terminal; developing automatic login procedures that circumvent the manual entry of the account's username and password; or allowing anyone to use the account).
(3) I will notify the 53 CSS when the account is no longer needed, account information needs revising, or the account password has been knowingly compromised.
(4) The account will be used in accordance with all existing regulations, policy directives, and guidelines to ensure no improper or fraudulent use.
(5) I will immediately notify my IAO in the event I am exposed to information to which I am not authorized or if I become aware of any security deviation.

Furthermore I understand that:
(1) Data and files associated with this account are subject to random review.
(2) The account password will be changed at least once every 90 days.
(3) I am responsible for not only safeguarding the classified contents of this account, but also the physical configuration of the network.

Applicant Signature	Date:

B. Security Officer Certification

1. As the Security Representative, I certify the "Applicant is accessed, per AFADS, to Lofty Trail (LTR)". I agree to notify the CAFNET Information Assurance Manager (IAM) upon any suspension of access of the applicant. If the applicant is a contractor, I further certify that sections 10e1 and 10f of the contractors DD Form 254 reflect the correct information for access to requested network connection.

Printed Name	Signature	Date

C. IAO INFORMATION: **I certify that the applicant has received initial computer security and network training. I agree to notify the CAFNET Information Assurance Manager (IAM) upon any suspension of access of the applicant.**

Encryptor RED IP Address:

Client IP RED Address(es):

RED IP not required for ISS and SGN

Contractors: Enter the PID's your LAN is approved for: GOV Disregard

Phone: **E-mail:**

IAO's Printed Name	IAO Signature	Date

D. PSO Certification

I certify that:
(1) The applicant requires access to AFADS in the performance of his/her duties.
(2) This account will be used in support of an official DoD project/contract.
(3) It is my responsibility to re-evaluate the need for this account and I will notify 53 CSS when the account is no longer needed.
(4) The PID's listed by the IAO are authorized on this system.

Printed Name	Title:
Signature	Date

Continuation for user: First Name: Last Name:

E. AFADS Specific Information:

IAO PROVIDES THIS INFORMATION

☐ AFADS - SPAWN ☐ AFADS - CDS ☐ New Account / New Node ☐ New Account / Existing Node ☐ Modify Node

☐ AFADS - PJ ☐ AFADS - ISS ☐ Existing Account / Additional Node ☐ Modify Account

ISS User Name:

USER/IAO PROVIDES, PSO VERIFIES THIS INFORMATION

Roles

☐ Security Officer ☐ Security Officer Read Only ☐ Air Staff ☐ PSO/CAO ☐ *Help Desk* ☐ *Sys Admin*

The privileges listed below are those for which not everyone will have access based on roles. If the default setting for your role is insufficient check the add-on role you require and justify the requirement in the comment section. Default settings are identified in the attached matrix.

Core Privileges

Person

☐ Admin
Archive Personnel records (only deceased/SSANs)

☐ *Sensitive*
View people whose existence in AFADS has been deemed a sensitive fact

VR

☐ *View All*
View any Visit Request in system

Network

☐ ACE
Ability to flag PID(s) authorized on a given network.

☐ SGN
Ability to flag PID(s) authorized on a given network.

☐ *ACE Adjudicator*
Ability to flag personnel for inclusion of data in the network adjudicator file.

☐ *SGN Adjudicator*
Ability to flag personnel for inclusion of data in the network adjudicator file.

Administrative Privileges

☐ Node Modify
Make changes to a node's profile (which programs may be viewed, users, etc.)

☐ Prog. Modify
Change attributes of a program.

☐ User Modify
Change a user's acount profile

☐ MOTD Admin
Add or modify message of the day (MOTD)

☐ MOTD Admin. View
View details on when/who created or modified an MOTD

☐ Org. Modify
Add, modify or archive organizations

☐ Network Admin.
Establish/change details for crypto, add/change IP addresses, produce router tables

☐ Network Admin. View
User can view details on crypto, networks.

☐ Comment Admin.
Add adminstrative remarks/user feedback, change status of submitted comments

☐ Comment Admin. View
View details on when/who created or modified a comment, admin notes, and feedback.

☐ System
When combined with the Network Admin privilege; configure routers and/or crypto.

☐ Lookup View
Ability to view (or modify) lookup tables (e.g., titles, Sponsor Orgs, etc.)

☐ Lookup Modify
Ability to view (or modify) lookup tables (e.g., titles, Sponsor Orgs, etc.)

Other: ☐ *UNIVERSAL LOG-ON*
Allows Log-On from any node.

General Privileges

General

☐ View All Programs
View data on all programs in the system, regardless of whether or not the user is accessed to it (if a user lacks this privilege they can only view access information for programs they are accessed to).

Audit

☐ Node (Users on same)
Audit other users that have logon privileges at that node

☐ Std reports
Audit which reports a user has run (and the criteria they set for a given report)

Reports

☐ Org Totals by Person
Provides a count, by Org, based on selected criteria.

☐ User Privilege
List users with a specified privilege (or combination of privileges).

☐ Person Boolean
Compose a custom query on the spot. Searchable fields are from Personnel and access record.

☐ Waiver
List people granted a waiver (along with approver/date and organization)

☐ AAA
Lists who has acted as AAA for a given program

☐ Annual
Used by Air Staff for annual Congressional reporting (single program)

☐ Annual One-click
Used by Air Staff for annual Congressional reporting; includes all programs designated as 'Umbrella'

☐ Clearance Variance
For a specified program, lists accessed people with a current clearance below the level they are accessed to

☐ Export All (Personnel)
Ability to extract personnel records for a specified organization

☐ Node
List information about nodes (e.g., users, approved programs, etc.)

☐ Non-US Citizen
List foreign nationals that are accessed to specified program(s).

☐ Org Totals by Access
List all organizations that have people assigned that meet search criteria, and the # of people accessed for those orgs.

Comments:

AFADS PSO Name | Title:

AFADS PSO Signature: | Date:

PRIVACY ACT STATEMENT

AUTHORITY: 10 USC 8013, 10 USC 974, 5 USC 301.
PRINCIPAL PURPOSE: To accurately identify personnel who require access to classified information resident on CAFNET and CAFNET services.
ROUTINE USES: Verification of personnel
WHETHER DISCLOSURE IS MANDATORY OR VOLUNTARY AND EFFECT ON INDIVIDUAL OF NOT PROVIDING INFORMATION: Disclosure is voluntary. However, access to CAFNET information may be denied with out the information on this form.

Instructions for completing CAF form 21a "AFADS Account Application".

This form is designed to be filled out on-line, printed then faxed or sent via CASTS messaging.

NOTE: Fax the completed form to DSN: 872-8834, Comm: 850-882-8834 (auto answer); or DSN: 875-2289, Comm: 850-883-2289 . Forms may also be sent using CASTS messaging to: FORMS,ContrCAF53CSS.

Section - A: The Applicant or the Information Assurance Officer (IAO) fills in the applicant's personal information. After reading the certification the applicant signs the form.
Section - B: The Security Officer (GSSO, CPSO) signs this section certifying that the individual has been entered into AFADS and is cleared to LTR.
Section - C: The IAO provides the red IP address requested, their e-mail address and phone number where they can be contacted at. The red IP's are not required if requesting AFADS over SGN/CDS or ISS. The PID's authorized for the LAN from which you are making the AFADS connection from. i.e. SPAWN-A, etc.
Section - D: The PSO for the unit the applicant belongs to signs in this section; certifying the need for the AFADS account.

At the top of page two there is a place to enter the applicants first and last name. This should be filled because sometimes when the forms are faxed the pages get separated.

Section - E: This area provides the information needed to establish the account. The IAO provides the information in the top block by checking the boxes that apply. If the account requested is for connection through ISS, the ISS user name must be supplied.

The second block is completed by the user/IAO and the PSO that signed the front of the form in section "D". verifies the need. Should these areas: (Help Desk, Sys Admin, (under Roles), Sensitive (under Person), View All (under VR), ACE and SGN Adjudicator (under Network) and UNIVERSAL LOG-ON) be checked the form must be signed at the bottom of section "E" by the appointed AFADS PSO.

NOTE:
1) This matrix depicts default privileges associated with given role; particular privleges may be added or deleted on a case-by-case basis.
2) If Security Officer Read Only is chosen the applicants account will not receive the privileges noted by a blue * .

ROLE	Security Officer	PSO/CAO	Air Staff	Help Desk	System Admin
CORE PRIVILEGES	**CORE PRIVILEGES**	**CORE PRIVILEGES**	**CORE PRIVILEGES**	**CORE PRIVILEGES**	**CORE PRIVILEGES**
Person	**Person**	**Person**	**Person**	**Person**	**Person**
View	X	X	X	X	X
Modify (incluses add)	*	X	X	X	X
Admin			X	X	X
Foreign National	*	X	X	X	X
Sensitive		X	X		X
Foreign Travel	*	X	X	X	X
Accesses	**Accesses**	**Accesses**	**Accesses**	**Accesses**	**Accesses**
View	X	X	X	X	X
Modify	*	X	X	X	X
Par's	**PAR's**	**PAR's**	**PAR's**	**PAR's**	**PAR's**
View	X	X	X	X	X
Modify (includes create)	*	X	X	X	X
Visit Requests	**Visit Requests**	**Visit Requests**	**Visit Requests**	**Visit Requests**	**Visit Requests**
View	X	X	X	X	X
Modify	*	X	X	X	X
Create	*	X	X	X	X
View All		X		X	X
Reports	**Reports**	**Reports**	**Reports**	**Reports**	**Reports**
AAA		X	X	X	X
Annual		X	X	X	X
Annual On-click			X		X
Clearance Variance		X	X	X	X
Common Access	X	X	X	X	X
Export (Personnel)	X	X	X	X	X
Export All (Personnel)					X
Hierachy	X	X	X	X	X

ROLE	Security Officer	PSO	Air Staff	Help Desk	System Admin
CORE PRIVILEGES	**CORE PRIVILEGES**	**CORE PRIVILEGES**	**CORE PRIVILEGES**	**CORE PRIVILEGES**	**CORE PRIVILEGES**
Reports	**Reports**	**Reports**	**Reports**	**Reports**	**Reports**
Local Records Check	X	X	X	X	X
Node				X	X
Non-US Citizen		X	X	X	X
Org Roster	X	X	X	X	X
Org Totals by Access Org		X	X	X	X
Totals by Person		X	X	X	X
Person Boolean			X	X	X
Program Roster	X	X	X	X	X
Program Totals	X	X	X	X	X
Program Standard	X	X	X	X	X
Quota	X	X	X	X	X
Security Training	X	X	X	X	X
User Privlege				X	X
Visit Request	X	X	X	X	X
Waiver Report		X	X	X	X
GENERAL PRIVILEGES	**GENERAL PRIVILEGES**	**GENERAL PRIVILEGES**	**GENERAL PRIVILEGES**	**GENERAL PRIVILEGES**	**GENERAL PRIVILEGES**
General	***General***	***Genera***	***General***	***General***	***General***
Comment Create	X	X	X	X	X
MOTD View	X	X	X	X	X
Org View	X	X	X	X	X
View All Programs		X	X	X	X
Audit	***Audit***	***Audit***	***Audit***X	***Audit***X	***Audit***
Basic (Self-Audit)	X	X	X	X	X
Node (Users on same)		X	X	X	X
System (all users)	X	X		X	X
Std Reports		X	X	X	X
E-Files	***E-Files***	***E-Files***	***E-Files***	***E-Files***	***E-Files***
View	Not Avail (post PL3)	Not Avail (post PL3)	Not Avail (post PL3)	Not Avail (post PL3)	Not Avail (post PL3)
Modify	Not Avail (post PL3)	Not Avail (post PL3)	Not Avail (post PL3)	Not Avail (post PL3)	Not Avail (post PL3)
Tier	***Tier***	***Tier***	***Tier***	***Tier***	***Tier***
Tier 1	CAO/Tier 2 managed	CAO/Tier 2 managed	CAO/Tier 2 managed	CAO/Tier 2 managed	CAO/Tier 2 managed
Tier 2	CAO managed	CAO managed	CAO managed	CAO managed	CAO managed
Tier 3 (Adjudicator)	CAO managed	CAO managed	CAO managed	CAO managed	CAO managed
Tier 3 Manager	CAO managed	CAO managed	CAO managed	CAO managed	CAO managed
Tier View	X	X	X	X	X
Network	***Network***	***Network***	***Network***	***Network***	***Network***
ACE	By Exception only. Must provide justification.	By Exception only. Must provide justification.	By Exception only. Must provide justification.	X	X
SGN/CDS				X	X
ACE Adjudicator	By Exception only. Must provide justification.	By Exception only. Must provide justification.	By Exception only. Must provide justification.	X	X
SGN/CDS Adjudicator				X	X
ADMIN PRIVILEGES	**ADMIN PRIVILEGES**	**ADMIN PRIVILEGES**	**ADMIN PRIVILEGES**	**ADMIN PRIVILEGES**	**ADMIN PRIVILEGES**
System Administration	***System Administration***	***System Administration***	***System Administration***	***System Administration***	***System Administration***
Node View	X	X	X	X	*X*
Node Modify	BY Exception	BY Exception	BY Exception	X	X
Program View	X	X	X	X	X
Program Modify	By Exception	By Exception	By Exception	X	X
User View	X	X	X	X	X
User Modify	By Exception	By Exception	By Exception	X	X
MOTD Admin	By Exception	By Exception	By Exception	X	X
MOTD Admin View	By Exception	By Exception	By Exception	X	X
Org Modify	By Exception	By Exception	By Exception	X	X
Network Admin	By Exception	By Exception	By Exception	X	X
Network Admin View	By Exception	By Exception	By Exception	X	X
Comment Admin	By Exception	By Exception	By Exception	X	X
Comment Admin View	By Exception	By Exception	By Exception	X	X
System	By Exception	By Exception	By Exception	X	X
Lookup View			X	X	X
Lookup Modfy	By Exception	By Exception	By Exception	X	X
UNIVERSAL LOGON	For PSO's Sys Admins; by exception for all others	For PSO's Sys Admins; by exception for all others	For PSO's Sys Admins; by exception for all others	For PSO's Sys Admins; by exception for all others	For PSO's Sys Admins; by exception for all others

Questions concerning forms processing call Jim Murray (850) 883-2668. For questions on account maintenance call (850) 882-8128.
Questions concerning role matrix and access should be directed to Mr. Jake Bronkema (781) 266-0896, DSN: 845-0896.