

USER AND E-MAIL ACCOUNT

1. LAST NAME		2. FIRST NAME		3. MIDDLE INITIAL	4. RANK/CIV GRADE	5. OFFICE SYMBOL
6. POST LOCATION	7. DUTY PHONE 6-	8. NAME OF SOMEONE IN OFFICE/PERSON BEING REPLACED			9. INFORMATION AWARENESS TRAINING DATE (YYYYMMDD)	
10. STUDENT HIRE <input type="checkbox"/> YES <input type="checkbox"/> NO		11. DMS REQUIRED <input type="checkbox"/> YES <input type="checkbox"/> NO		12. DISTRIBUTION LISTS		13. SECURITY GROUPS
14. SECURITY CLEARANCE/SIGNATURE OF SECURITY MANAGER/306 FORM				15. SIGNATURE OF INFORMATION SYSTEM SECURITY OFFICER(ISSO)		

PASSWORDS (REF: AFMAN 33-223, paragraphs 3.4., 4.2., and 4.6.)
 I understand that my password must be a minimum of eight (8) characters, alpha-numeric, and contain special characters. My password **will not** be written down or given to any other person. When I no longer need access to the network and/or when I leave my computer, I will log out of the network and my screensaver will be password protected as well.

NEVER GIVE OUT YOUR USER ID AND/OR PASSWORD!

WORLD WIDE WEB POLICY (REF: AFI 33-129, paragraph 6.1.)
 Accessing the Internet through a government computer is using a government resource. Government provided hardware and software are for conducting official and authorized government business. This does not prohibit commanders from authorizing personnel to use government resources to further their professional and military knowledge if they determine it is in the best interest of the government and authorization is documented by letter, local operating instruction, or explicit policy. Using the Internet for other than authorized purposes may result in adverse administrative or disciplinary action.

SYSTEM MONITORING (REF: AFI 33-202, Vol 1, paragraph 3.10.)
 I agree to use this government computer system for authorized use only. Computer systems may be monitored for all lawful purposes, including to ensure that their use is authorized, for management of the system, to facilitate against unauthorized access, and to verify security procedures, survivability, and operational security. Using this system constitutes consent to monitoring. All information, including personal information, placed on or sent over this system may be obtained during monitoring. Unauthorized use could result in adverse administrative, disciplinary action and/or prosecution.

VIRUS PROTECTION (REF: AFI 33-202, paragraphs 3.8.3.2. and 3.8.3.3.)
 Virus scans are crucial to network protection. HQ ARPC has implemented that a virus scan must be conducted on fixed media (i.e., hard drives) on a weekly basis. Virus scans on removable media (i.e., floppy disks) must be conducted before each use.

I HAVE READ AND UNDERSTAND THE ABOVE INFORMATION

16. SIGNATURE	17. DATE SIGNED (YYYYMMDD)
---------------	----------------------------

FOR NCC USE ONLY

18. USER ID		
19. COMMENTS		
20. DATE SENT TO HELPDESK (YYYYMMDD)		
21. IA TECHNICIAN	22. SIGNATURE	23. DATE (YYYYMMDD)

**Download any U.S. FedForm (free, fillable, savable in Adobe Reader)!
Start with the "Flash Demo" at the top of the following page:
www.usa-federal-forms.com**

**Convert any fillable PDF form to savable (locally, in Adobe Reader):
www.savePDF.com**

**Convert any document (in any format) to PDF fillable and savable:
www.FillinDocs.com**

**All (10's of 1,000's) U.S. Federal Forms already fillable, savable:
www.usa-federal-forms.com**

About the ITAOP/savePDF Method

The traditional Field-by-Field creation process is extremely ineffective and slow.

The only realistic option to create high-quality forms is the Insert-Text-Anywhere-on-Page (ITAOP) method.

The field creation process is about 10,000 times faster than the traditional method; the list of ITAOP features is not even available for the traditional method.

ITAOP savePDF method proved to be very simple and completely reliable for millions of users all over the world (incl. individuals, companies, organizations, government employees).