

**BY ORDER OF THE  
SUPERINTENDENT**

**HQ UNITED STATES AIR FORCE ACADEMY  
PAMPHLET 33-109**

**19 November 2003**

**Communications**

**COMPUTER USER STARTER KIT**



---

**NOTICE:** This publication is available digitally on the AFDPO WWW Site at:  
<http://afpubs.hq.af.mil>

---

OPR: 10 CS/SCBN (1st Lt Brian Holinka) Certified by: 10 CS/SCB (Major Michael J. Polley)  
Supersedes USAFAPAM 33-109, 10 April 2001

Pages: 19

Distribution: F

---

The purpose of this pamphlet is for use as a guide to assist users in becoming productive and responsible network citizens, locating the proper authoritative or regulatory guidance on computer use and procedures, as well as specific issues dealing with the United States Air Force Academy (USAFA) network. It is not directive in nature; that is the function of the source document or reference. It is the computer user's responsibility to be familiar with the source documents referenced throughout the publication. This pamphlet will not necessarily address every topic or issue you may have. This pamphlet is applicable to all USAFA computer network users.



**TABLE OF CONTENTS**

Welcome .....	Chapter 1
How to Get Help .....	Chapter 2
Air Force Guidance.....	Chapter 3
USAF Hardware and Software Standards.....	Chapter 4
Training.....	Chapter 5
The USAFAnet Local Area Network .....	Chapter 6
Getting Started on USAFAnet .....	Chapter 7
Electronic Mail (E-mail).....	Chapter 8
Computer Crime.....	Chapter 9
Computer Viruses and Protection .....	Chapter 10
USAFAnet Security Training .....	Chapter 11
USAFAnet User Agreement .....	Attachment 1
Personal Digital Assistants .....	Attachment 2

## Chapter 1

### WELCOME

**1. Welcome.** Welcome to the United States Air Force Academy (USAFA). We compiled this “starter kit” with the new USAFA computer user and USAFA network (USAFAnet) customer in mind. The information contained in this guide will get you on your way to becoming a productive and responsible network citizen. Don’t be dismayed if some of the information contained in this pamphlet is too technical or confusing. You can become a productive network user and personal computer user without being a so-called “geek”. On the other end of the spectrum, some users may find much of this information trivial and not the least bit challenging. Good for you! However, whether you’re a novice or a full-fledged computer geek, all USAFAnet users are responsible for knowing and understanding the basic rules and guidelines contained in the applicable Air Force Instruction (AFI) and USAFA supplements. We’ve condensed the really important stuff here. In fact, after you read about your responsibilities in the arenas of software privacy, virus protection, and computer security, you’ll be asked to sign the attached Network User License form acknowledging your understanding and willingness to abide by these “rules of the road.” We’re confident you’ll find being a responsible network citizen an easy thing, indeed a good thing, to do. However, Internet communications are monitored and evidence of inappropriate usage will be reported to individual commanders for appropriate action. Your written consent to monitoring is a mandatory requirement for getting or maintaining your USAFAnet accounts. Your Workgroup Manager (WM) is responsible for maintaining signed USAFAnet agreements. An agreement example is provided at the end of this document.

## Chapter 2

### HOW TO GET HELP

**2. How to Get Help.** A comprehensive guide to all the “ins” and “outs” of USAFAnet and your PC software applications would take many, thick volumes. That’s certainly not the purpose of this guide. Instead, this booklet is here just to get you started.

2.1. We expect you’ll have questions. Your WM is the place to start in your search for answers. The 10th Communications Squadron (10 CS) Help Desk is your next step. The Help Desk is located in room 2J7 in Fairchild Hall, right out the door of the south elevator on the second floor. It’s designed to be your “one-stop-shop” for all your communications and information needs. Personnel are on duty from 0700 to 1630 Monday through Friday. You can reach our Help Desk by dialing 3-HELP (3-4357), or by simply sending an electronic message (e-mail) to [SC\\_helpdesk@usafa.af.mil](mailto:SC_helpdesk@usafa.af.mil). Extended customer support via telephone is available from 0600-0700 and 1630-2300 every day during the school year and 0600-0730 during spring, summer, and winter breaks; dial 3-HELP. After hours, Help Desk personnel perform standby duty and assist with Emergency outages. Contact the after-hours technician at 338-5799, between 2300-0600, Monday-Friday, and all day Saturdays and Sundays.

2.2. The Help Desk exists to provide information about the full range of network and computer services provided by the 10 CS. Information includes hardware and software support and advice for your computer workstation, as well as USAFAnet connectivity and usage. That’s a lot of ground to cover, which is why the Help Desk technician may not always be able to answer your question without referring you to an expert in that specific area. We will make every effort to help you as much as possible and solicit your feedback via the customer satisfaction survey. Tell us where we’re doing things right, and let us know how we can improve.

## Chapter 3

### AIR FORCE GUIDANCE

**3. Air Force Guidance.** There are a number of Air Force Instructions that govern how each of us should use the computing resources in our workplace. The most important guidance for USAFAnet users include AFI 33-119, *Electronic Mail (E-Mail) Management and Use*, AFI 33-129, *Transmission of Information via the Internet*, and AFI 33-202, *Network and Computer Security*, and their respective supplements. Make sure you're familiar with the contents of these publications.

3.1. The USAFA Configuration Control Board (CCB) establishes additional policies for future inclusion in a USAFA supplement. You will be advised when new policies are established. All of them will be stored in the Y:\USAFANET\POLICIES directory on USAFAnet.

## Chapter 4

### USAFA HARDWARE AND SOFTWARE STANDARDS

**4. USAFA Hardware And Software Standards.** Over 9,000 computer users live and work at the Academy. In order to support such a massive user-base economically and efficiently, it is imperative that we establish and enforce a number of hardware and software standards. These standards are published in the *USAFA C4 Standards Guide* which is stored in Y:\USAFANET\POLICIES\STDGUIDE.DOC.

4.1. For most users, all you need to know is that the standard desktop computer is a Microsoft Window personal computer (PC) (as opposed to a Macintosh, for example), and we provide and support the Microsoft Office suite of application software. That includes Word (word processor), Excel (spreadsheet), PowerPoint (presentation software), and Access (relational database management system). These powerful software packages are used throughout business, industry, and academia (and the Air Force for that matter!). Depending on the task, each can make it easier for you to perform your job.

4.2. To assist you in keeping your computer updated with the latest security patches; Systems Management Server (SMS) will automatically load these on your machine. SMS will also be used to assist you with computer problems without having to leave your desk. SMS will be used only when either the customer or WM is present at the PC and will never be used to conduct unlawful searches.

4.3. Your office or organization may use other software specific to your mission. Two types of software that need to be identified and approved before usage are Shareware and Freeware. Shareware is software that the creator allows you to try for a period of time and is removed once the time is up, if you don't purchase it. Freeware is software that the creator allows you to use at no cost and doesn't have a termination date. Both of these types of software have to be approved by the Designated Approving Authority (dual-hatted as Headquarters USAFA Senior Communicator (HQ USAFA/SC) and the Commander of the 10th Communications Squadron (10 CS/CC) on the Academy) before you use them. Your WM or supervisor will inform you about those packages and provide any additional training you may require.

4.4. Personal Digital Assistants (PDAs), both personally and government owned, are authorized for use; however, users must adhere to the requirements of AFI 33-202, *Network and Computer Security*, paragraph 4.3.3. Additionally, PDA users connecting to USAFAnet shall complete the PDA Registration form found at Attachment 2.

## Chapter 5

### TRAINING

**5. Training.** Many people are already familiar with these specific software programs. Others have previously used similar software. Changing to a different product is usually not difficult. However, if training is needed to make the transition or you have no experience with a particular type of software, there's no reason to despair.

5.1. Computer-Based Training (CBT) is available to all USAF personnel (active duty, Air National Guard (ANG), Air Force Reserve Command (AFRC), and civilians) assigned to the Academy. It is located on the USAFA Intranet at <http://intraweb.usafa.af.mil/sc/scb/scbnl/cbt/>.

5.2. There is also valuable information and tips located on the Help Desk web page <http://intraweb.usafa.af.mil/scbnc/index.html>.

5.3. The <http://intraweb.usafa.af.mil/scbnc/netstat/index.html> site displays a status of all major network functions.

5.4. 10 CS offers additional computer and network training, primarily for WMs and Network Control Center (NCC) personnel; however, base-wide users are encouraged to sign up for in-house offered courses on a stand-by basis. Check the NCC Training Element web site for upcoming classes, class description, and class dates. The web site address can be reached at: <http://intraweb.usafa.af.mil/sc/scb/scbnl/>.

5.5. The 10 CS will also provide references to commercial contractors for training on all standard software packages. It is each unit's responsibility to schedule and fund their training. Remember, your unit bears the cost of this training, so be sure to clear it with your boss before you sign up.

## Chapter 6

### THE USAFAnet LOCAL AREA NETWORK

**6. The USAFAnet Local Area Network.** A Local Area Network (LAN) is a convenient and efficient way to connect groups of workstations. USAFAnet is the LAN for the Air Force Academy.

6.1. USAFAnet is a Windows NT network. (NT is the network operating system (NOS)) NT networks may have anywhere from one to hundreds of servers connected together. Here at the Academy, USAFAnet is composed of over 50 servers. A server is a computer that manages the network and many of its resources. An NT server supports and manages these key features:

- **Software Services** manage the way workstations operate on the LAN and how all network resources are used.
- **NT services** make it possible for you to:
  - Share files
  - Share printers
  - Use e-mail and other network software
- **Communications Options** make it possible for you to use your workstation as a terminal connected to different host computers and to access outside information services and databases.
- **Hardware Services** allows you to access and share many hardware resources including:
  - Printers
  - Network Drives
  - Workstations
  - Other computers
  - Other servers

6.2. Your WM can help you configure your computer to map the printer or printers you need to do your job. There are self-help instructions located at the following website: <http://intraweb.usafa.af.mil/scbnc/netstat/TCP%20IP%20Printing.html>. They can also explain the use of the shared network drives. Your WM is responsible for allocating disk space on your shared drives. Remember, it is best to keep large files off the shared drives or you may exceed your authorized disk space.

6.3. The USAFAnet Wireless Area Network. The Wireless Area Network (WAN) was established to assist cadets in using laptops in various locations around the campus. There are a number of security concerns with the WAN, so you need to be aware of certain procedures to utilize this service. All access points or other equipment to be used

on the WAN must be approved by the CCB. Dual connections (simultaneous connection to the wired and wireless networks) as well as peer-to-peer links are not permitted. Your WM or supervisor will be able to answer any questions or provide any additional training you may require.

## Chapter 7

### GETTING STARTED ON USAFAnet

7. **Getting Started on USAFAnet.** Your WM will submit a request to establish a USAFAnet account for you. You then need to log in and set up your account. That means resetting your password to a unique one for you. When a computer connected to USAFnet boots up, you will be asked to provide your user name and password.

7.1. Your user name identifies you whenever you login to USAFAnet. The format is established in AFI 33-119, where your username is **firstname.lastname**. For example, Col John Smith's user name is **john.smith**. The naming convention for cadets is **cyyfirstname.lastname**. The **cyy** denotes the class year. Cadet John Smith from the Class of 2001 would have a user name: **c01john.smith**.

7.2. Next, you will be prompted for your password. Your WM will provide an initial one that must be changed upon first logon. You should **immediately** reset it. Your password must be at least eight (8) characters and contain a combination of upper case, lower case, special characters, and numbers. Choose a password that is NOT a commonly used word or a name that can be easily associated with you, such as your spouse's or child's name, a favorite color, or aircraft. You can find helpful guidance on selecting and maintaining passwords on the web page: <http://intraweb.usafa.af.mil/scbnc/accounts/index.html>.

7.3. Most critical, PROTECT your password. NEVER give it out to anyone. If anyone asks for your password, refuse them and call your WM. (USAFAnet system administrators will NEVER request your password.) Do not leave it written down near your work area. Armed with your password, anyone can log in as YOU. Any activity performed from your account is YOUR responsibility.

7.4. Your USAFAnet password will expire in 90 days. The system keeps track of your previous passwords and will not let you change a password to one used before. An error message will appear if you try to use an old password. You must make each new password unique.

7.5. Password-protected screen savers are mandatory for all computers attached to USAFAnet. Screen-savers must be configured to come on after at most 15 minutes. The unit commander may set local policy that lowers this time limit. We strongly recommend local policy be set to a 5 minute limit. If someone uses your computer for an unauthorized purpose while you are logged on, you will be held accountable.

## Chapter 8

### ELECTRONIC MAIL (E-mail)

**8. E-mail.** If you're like most users, e-mail will be your single biggest use of the LAN. As a USAFAnet user, you're capable of sending and receiving e-mail not only to and from your fellow USAFAnet users, but to and from others worldwide via the Internet. The e-mail package currently in use at the Academy is Microsoft Outlook 97/98/2000/XP. Here are answers to three frequently asked questions:

#### 8.1. How do I send an e-mail?

To send e-mail messages to someone on base, simply click on the TO button in the new message. This will display the address list. You can select the address from there.

To send messages off base (Internet mail), type in the entire e-mail address. For example,

john.smith@langley.af.mil, jane.doe@uswest.net

#### 8.2. What is my e-mail address?

For someone to e-mail you from off base, they simply address the message to your user name firstname.lastname@usafa.af.mil. For example, John Smith's address is john.smith@usafa.af.mil

#### 8.3. What is the file size limit to sending or receiving an attachment with my e-mail?

You may send or receive an e-mail attachment that is no larger than 10 MB.

## Chapter 9

### COMPUTER CRIME

**9. Computer Crime.** Some people who would never walk into a store and shoplift a software product think nothing of making several copies of that same software and distributing them to friends and colleagues. The results are the same. The act is just as wrong and just as illegal.

9.1. Softlifting. Softlifting is the term applied when individuals illegally make copies of licensed software for their own use or use by a friend. Most softlifters see themselves helping a friend and don't realize a crime is being committed that hurts not only the software developer but the customer community as well.

9.2. Software piracy. Software piracy occurs when organizations choose consciously to encourage or unconsciously to allow employees to make and use illegal software copies. Both practices violate the US copyright law and expose the individuals and companies involved to significant fines and even jail terms.

9.3. The law is clear. Reproducing computer software without authorization violates the US copyright law. It is a federal offense. The money paid for a software product represents a license fee for the use of one copy. It does not represent an authorization to copy and redistribute. Civil damages for unauthorized software copying can be severe and criminal penalties can include fines and imprisonment. USAFA conducts software scans to ensure lawful compliance.

9.4. Additionally, downloading, storing on network resources, and redistributing copyrighted material including, but not limited to, music, movies, and written material, without proper authorization from the intellectual rights owner may infringe on US copyright law and violates AFI 33-129.

## Chapter 10

### COMPUTER VIRUSES AND PROTECTION

**10. Computer Viruses and Protection.** A computer virus is a program which replicates itself without a user's knowledge. Some are relatively harmless, simply a nuisance. Others can result in total loss of data, even the complete reformatting of a disk drive. They can be spread through a variety of ways including shared diskettes, the Internet, Bulletin Board Systems, etc. Viruses cannot be transmitted by reading e-mail or receiving e-mail with an attachment. But an e-mail may have an infected attachment! If an infected e-mail attachment is opened, a virus could infect your entire computer system and propagate to other systems.

10.1. The only way to absolutely protect a system from viruses is to not have any contact with any other systems whatsoever; however, a good antivirus (AV) program installed on your computer provides reasonable protection. The Academy mandates using the Norton Antivirus program. Air Force Special Security Memorandum (SSM) 5023 requires that all users have current AV software on their machines. Your WM is responsible for verifying AV software is installed and configured properly. Your AV software shall be set to managed, which updates automatically. Contact your WM for assistance in having this performed automatically.

## Chapter 11

### USAFAnet SECURITY TRAINING

#### 11.USAFAnet Security Training.

##### 11.1. Why Computer Security Training?

- Directed by the Air Force
- Makes all of us better network citizens
- Knowledge of and adherence to the policies and instructions governing network use protects valuable Air Force investments: network infrastructure and components, and you!

##### 11.2. Go to the Source

As mentioned earlier, the Air Force has published two specific instructions that serve as our guidelines for proper network use:

- AFI 33-119, *Electronic Mail (E-Mail) Management and Use*, and the USAFA Supplement
- AFI 33-129, *Transmission of Information via the Internet*, and the USAFA Supplement

##### 11.3. Every USAFAnet User Must Know and Practice the following “rules of engagement” for:

- Appropriate use of the Internet
- Authorized use of e-mail
- Personal use of Internet and e-mail
- Password creation and protection
- Protection from computer viruses

##### 11.4. Appropriate Use of the Internet. Government-provided hardware and software are for conducting official and authorized government business. Using the Internet for other than authorized purposes may result in adverse administrative or disciplinary action.

Reference AFI 33-129, paragraph 6.1.

###### 11.4.1. AFI 33-129 paragraph 2. directs:

"The Internet provides opportunities for quick and efficient disseminating of information to the public, distributing information throughout the Air Force, and accessing information from a variety of sources. Information may be sent between offices or individuals or be displayed on the web. The Air Force goal for the Internet is to provide maximum availability at acceptable risk levels for Air Force members needing access for the execution of official business."

##### 11.5. The following activities are specifically prohibited:

- Any use that is not official or authorized government business.
- Activities for personal or commercial financial gain such as chain letters, commercial solicitation, and sales of personal property.
- Storing or processing classified information. (USAFAnet is not accredited for classified usage).
- Storing, processing, displaying, sending, or otherwise transmitting offensive or obscene language or material. Offensive material includes: “hate literature”, such as racist literature, materials or symbols (for example, swastikas, neo-Nazi material, and so forth), and sexually harassing materials. Obscene material includes, but is not limited to, pornography and other sexually explicit materials.
- Using another person’s account or identity without appropriate authorization or permission.
- Copying or installing software in violation of the license agreement.
- Participating in off-base “chat lines” or open forum discussion unless for official purposes and after approval by Public Affairs.
- Attempting to circumvent or defeat security-auditing systems without prior authorization.
- Using “peer-to-peer” software.
- Distributing copyrighted materials without consent from the copyright owner. Failure to maintain consent may violate federal copyright infringement laws and could subject the individual to civil liability or criminal prosecution.

#### 11.6. Authorized Use of E-mail

- E-mail is used to supplement or replace traditional mail, facsimile, telephone, and other messaging systems.
- Only use e-mail for official, authorized, and ethical activities.
- Use e-mail to transmit both formal and informal correspondence.
- Limit the total size of all e-mail to less than 10 MB, including attachments.
- Use of e-mail serves as consent to monitoring.
- You must have chain of command approval before you subscribe to an e-mail listserv.
- Basic standards for using e-mail are common sense, common decency, and civility.

11.7. Personal Use of the Internet and E-mail. Your commander or designated supervisor, who is a commissioned officer or civilian above GS-11, can permit some personal use of the Internet and communications using government e-mail systems in accordance with the following stipulations:

- The use does not adversely affect performance of duties.
- The use is of reasonable duration and frequency and, whenever possible, is conducted during personal time (non-duty hours).

- The use serves a legitimate public interest, such as improving morale or furthering professional skills or education.
- The use does not reflect adversely on the Air Force.
- The use does not overburden the communications system and does not create significant additional cost to the Air Force.

#### 11.8. Password Creation and Protection.

- Choose a password thoughtfully and protect it carefully.
- Refer to <http://intraweb.usafa.af.mil/scbnc/accounts/index.html> for hints on how to select a good password.
- Never give it out to anyone.
- Never leave it written down in your work area.
- If you think it may have been compromised:
  - Inform your WM
  - Change it IMMEDIATELY

#### 11.9. Protection from Computer Viruses

- Your computer must have the latest version of antivirus software loaded and running.
- Update to the latest antivirus signature file when notified using the link on <http://intraweb.usafa.af.mil/scbnc/software/index.html>.
- Virus scan any exchanged floppies or files downloaded from the Internet.

#### 11.10. Computer Security Starts With You!

- Never walk away from your computer while logged on to the network without evoking a password-protected screen saver or logging off.
- Any network activity originating from your USAFAnet account is YOUR responsibility.

**Attachment 1**  
**USAFA NETWORK ACCESS USER LICENSE AGREEMENT**



**USAFA Network (USAFAnet)**  
**Access User License Agreement**



In accordance with AFI 33-115, Volume II, *Licensing Network Users and Certifying Network Professionals*, every individual who has access to the Air Force network (af.mil) domain, specialized systems, and mission systems must be trained and licensed.

**Part 1. Network User Licensing (NUL) Internet/Computer Based Training (C/IBT) Requirement.** NUL training has been standardized in the NUL C/IBT course. Successful completion of this course satisfies DoD user certification, Air Force Information Awareness Program training, and Air Force Network Users Licensing.

Details on the training and licensing requirements and guidance on access to the training will be provided to the users by workgroup managers (WM).

**Part 2.** Local user training requirement listed below reflects local needs and concerns. Users must comply with guidelines established in AFI 33-129, *Transmission of Information Via the Internet*, section 6, for the authorized and prohibited use of the Internet, and AFI 33-119, *Electronic Mail (E-Mail) Management and Use*, section 3, for authorized and prohibited use of the government E-mail system.

The following are several excerpts from the AFIs that require noting (users are still responsible for all information within these documents and will be held accountable and could be prosecuted for violations).

Accessing the internet through a government computer or network uses a government resource. Government-provided hardware and software are for conducting official and authorized government business. The following are prohibited on government computer systems:

- Any use of government-provided computer hardware or software for other than official and authorized government business.
- Activities for personal or commercial financial gain.
- Storing, processing, displaying, sending, or otherwise transmitting offensive or obscene language or material. Offensive material includes, but is not limited to, "hate literature," such as racist literature, materials or symbols, and sexually harassing materials. **Obscene material includes, but is not limited to, pornography and other sexually explicit materials.**
- Storing or processing classified information on any system not approved for classified processing. Participating in "chat lines" or open forum discussion unless for official purposes.
- Attempting to circumvent or defeat security or auditing systems.
- Sending or receiving E-mail for commercial or personal financial gain using government systems.
- Intentionally or unlawfully misrepresenting your identity or affiliation in E-mail communications.
- Sending harassing, intimidating, abusive, or offensive material to, or about others.
- Using someone else's identity (UserID) and password without proper authority.
- Causing congestion on the network by such things as the propagation of chain letters, broadcasting inappropriate messages to groups or individuals, or excessive use of the data storage space on the E-mail host server.
- The installation of "Freeware" or "Shareware" software, including trial versions offered by vendors, without written authorization and approval from the 10<sup>th</sup> Communications Squadron (All requests to install "Freeware" or "Shareware" software, including trial versions, must be coordinated through the 10<sup>th</sup> Communications Squadron).

By signing this User License Agreement I hereby confirm I have completed the Network User Licensing C/IBT, understand the proper and authorized use of my government computer and any violation may lead to my prosecution under the UCMJ or civil law, and my access to the USAFAnet temporarily or permanently restricted.

\_\_\_\_\_  
 Print User Full Name/Rank/Unit Office Symbol

\_\_\_\_\_  
 Signature Date

\_\_\_\_\_  
 Print Workgroup Mgr Name/Rank/Office Symbol

\_\_\_\_\_  
 Signature Date

**DEPARTMENT OF THE AIR FORCE**

HEADQUARTERS UNITED STATES AIR FORCE ACADEMY

USAF ACADEMY COLORADO

Date: \_\_\_\_\_

MEMORANDUM FOR 10 CS/SCB

FROM: \_\_\_\_\_  
(Rank, Name, Office Symbol)

Subject: PDA Agreement

1. My signature below indicates I understand that my privately owned personal digital assistant (PDA), which is a similar-type PDA to government-approved PDAs, has been approved for use by the DAA on the USAFA network (USAFAnet). In addition to the requirements in AFI33-202, *Computer Security*, I agree to the terms, actions, and conditions contained in this memo.

2. I will:

- a. Maintain a password on my PDA in accordance with (IAW) AFI33-202.
- b. Only use my PDA to process unclassified, non-Privacy Act information.
- c. Maintain antivirus software and adhere to security standards and other operational requirements as applicable to government-issued PDAs.
- d. Remove all sensitive information prior to disposing of or transferring (selling) my PDA.
- e. Consent to monitoring of my PDA, since it is connected to a system that is subject to being monitored.
- f. Take prudent security measures to protect the USAFAnet from unauthorized access via my PDA and its docking port.

3. I understand my PDA is subject to being audited at anytime to determine if my PDA contains Privacy Act or classified information.

4. I understand that the process for sanitizing sensitive and classified information from my PDA may result in its destruction and I waive any and all claims for reimbursement for any damage or destruction.

5. I understand the 10 CS Help Desk will assist me with PC-related problems but repair of my privately owned PDA is my responsibility.

6. I understand that if at any time I fail to meet the conditions stated above, I will be required to remove my PDA's USAFAnet connection and submit it for data sanitization.

7. I understand the Air Force does not assume any liability for my PDA, regardless of circumstance. I understand that all data entered on my PDA while performing government business becomes the property of the US Government.

8. Device information:

a. Make & Model: \_\_\_\_\_

b. Serial number: \_\_\_\_\_

c. Operating system: \_\_\_\_\_

d. Installed software: \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

9. I can be contacted at:

\_\_\_\_\_

(phone number and office symbol)

Signature: \_\_\_\_\_

Signature Block: \_\_\_\_\_

File:

1 - Original: 10 CS/SCB

2 - Unit Information System Security Officer

3 - Individual

KRISTEN A. DOTTERWAY, Lt Col, USAF  
Commander, 10th Communications Squadron