

**1 JUNE 2005**



***Communications and Information***

***45TH SPACE WING ENTERPRISE  
NETWORK (ENTNET) POLICY***

**COMPLIANCE WITH THIS PUBLICATION IS MANDATORY**

---

**NOTICE:** This publication is available digitally on the AFDPO WWW site at:  
<http://www.e-publishing.af.mil>

---

OPR: 45 SCS/SCABA  
(Mr. Harold N. Campbell)  
Supersedes 45SWI 33-108, 10 August 2000

Certified by: 45 SCS/CC  
(Lt Col Dennis W. Lisherness)  
Pages: 14  
Distribution: F

---

This instruction implements AFD 33-1, *Command, Control, Communications, and Computers (C4) Systems*, 17 Sep 93; AFI 33-119, *Air Force Messaging*, 27 Oct 2004; and provides policy and procedures for ENTNet management, security, and usage. This instruction applies to all 45 SW Enterprise Network (ENTNet) users to include supporting activities and contractors who operate C4 systems attached to the 45 SW ENTNet. It also applies to Tenant, Air National Guard, and Air Force Reserve units (including military, civil service, and contractor personnel) supported by the 45th Space Wing. Direct questions or comments regarding the technical content of this instruction to the Base C4 Help Desk (45 SCS/SCABC, 494-2666), or Network Control Center (NCC) (45 SCS/SCABA, 494-1996).

Failure to observe the prohibitions and mandatory provisions of paragraphs **4.1.2.1**, **4.5**, **4.6**, **5.1.3**, and **5.2** is a violation of Article 92, Uniform Code of Military Justice (UCMJ). Violations by civilian employees may result in administrative disciplinary action without regard to otherwise applicable criminal or civil sanctions for violations of related laws.

***SUMMARY OF REVISIONS***

This document is substantially revised and must be completely reviewed. This instruction replaces all previous 45 SW Network Policies.

**1. Purpose and Scope.**

1.1. The 45 SW ENTNet is Sensitive but Unclassified, government-owned communications network used for the purpose of processing information for authorized or official government use. It is connected to both the Department of Defense (DoD) Non-Secure Internet Protocol Router Network (NIPRNet) and the commercial Internet.

1.2. The purpose of this document is to instruct users how to effectively and appropriately use the 45 SW ENTNet and to set policies regarding official and authorized use of the 45 SW ENTNet.

1.3. This instruction applies to users and accounts. System Program Office (SPO) and Program Management Office (PMO) systems (such as PC-III, JOCAS, etc.), connecting to the 45 SW ENTNet communications backbone, will also follow this policy regarding accessing Systems and Networks connected to the 45th Space Wing ENTNet.

## 2. Getting Started.

2.1. Authorized Access. ENTNet access is available to all authorized 45 SW personnel and tenants, to include military and government civilians as well as wing and tenant contractors. Access is available to tenant organizations based on their host-tenant agreement with the 45 SW. Wing and tenant contractors are granted access based on the terms of their contract and their service level agreements with the government. In all cases, access is granted to perform authorized and official DoD or governmental business only.

### 2.2. How to Get an Account.

2.2.1. Work Group Managers, where available, are the primary focal point for individuals requiring an account on the ENTNet and will assist in completion of a Department of Defense (DD) Form 2875 or subsequently approved form in use for system access provided by the Base C4 (Command, Control, Communications, & Computers) Help Desk (4-2666) or the customer's Information Systems Security Officer (ISSO). Contractors must send this request through their government representative, who in-turn will forward this request to the Base C4 Help Desk for processing.

2.2.2. Prior to requesting access, each customer must satisfy all of the following:

2.2.2.1. Complete the Online United States *Air Force (USAF) Information Assurance Awareness* Internet-Based Training (IBT), per Air Force Instruction (AFI) 33-204, Paragraph 18.5 & 18.6 offered through the Patrick AFB Extranet website [https://pafbweb.patrick.af.mil/index\\_int.htm?Submit=Continue](https://pafbweb.patrick.af.mil/index_int.htm?Submit=Continue), then print the completion certificate and forward a copy with your submitted request to the Base C4 Helpdesk for processing.

2.2.2.2. Have a favorable National Agency Check (NAC), Entrance National Agency Check (ENTNAC), or equivalent; the individual's security manager must certify this, in writing as detailed in part III of DD Form 2875.

2.2.2.3. A waiver letter, signed by their Commander may be sent to the Base C4 Helpdesk for processing, due to the timeframe required to process an investigation. This letter must be in compliance with AFI 31-501, *Personnel Security Program Management*.

2.2.2.3.1. Per DoD 5200.2-R Information Assurance Implementation, February 6, 2003.

**Table 1. Investigative Levels for Users with IA Management Access to DoD Unclassified Information Systems.**

<b>Investigative Levels for Users with IA Management Access to DoD Information Systems</b> <b>(Investigative Levels are defined in DoD 5200.2-R)</b> <b>-- The term Foreign Nationals (FN) refers to all individuals who are Non-U.S. citizens including U.S. military personnel, DoD Civilian employees and contractors --</b>					
<b>Limited Privileged Access - IT-I</b>					
<b>User Roles</b>	<b>FN (See Note)</b>	<b>U.S. Civilian</b>	<b>U.S. Military</b>	<b>U.S. Contractor</b>	<b>Conditions or Examples</b>
IAM (with no IA administrative privileges)	Not Allowed	NACI	NACLCL	NACLCL	None
IAO (with no IA administrative privileges)	Conditionally Allowed – NACLCL (equivalent)	NACI	NACLCL	NACLCL	FN: - With DAA written approval direct or indirect hires may continue as IAOs until replaced. Provided they serve under the immediate supervision of a U.S. citizen IAM, and have no supervisory duties.
Supervisor of IT-II or IT-I positions	Not Allowed	NACI	NACLCL	NACLCL	None
Administrator (with no IA administrative privileges)	Allowed NACLCL – (equivalent)	NACI	NACLCL	NACLCL	Examples: - AIS administration, OS administration of common applications such as email, word processing. FN: - Under the immediate supervision of a U.S. citizen. All: - Also subject to IA Controls (e.g., PERF)

Investigative Levels for Users with IA Management Access to DoD Information Systems (Investigative Levels are defined in DoD 5200.2-R) -- The term Foreign Nationals (FN) refers to all individuals who are Non-U.S. citizens including U.S. military personnel, DoD Civilian employees and contractors --					
Limited Privileged Access - IT-I					
User Roles	FN (See Note)	U.S. Civilian	U.S. Military	U.S. Contractor	Conditions or Examples
Administrator (with IA administrative privileges)	Conditionally Allowed – SSBI – (equivalent)	SSBI	SSBI	SSBI	Examples: Administration of IA devices (e.g., boundary devices, IDS, routers and switches)  FN: – Under the immediate supervision of a U.S. citizen, and with written approval of the Head of the DoD Component
Maintenance of IA products	Conditionally Allowed – SSBI – (equivalent)	SSBI	SSBI	SSBI	FN: – Under the immediate supervision of a U.S. citizen, and with written approval of the Head of the DoD Component  All: - Also subject to IA controls (e.g., PEPF and ECRB)
<b>NOTE:</b> FN direct and indirect hires covered by the provisions of a Status of Forces Agreement (SOFA), or other international agreement, require host-nation personnel security investigations that are the equivalent of the U.S. investigative level indicated.					
<b>NOTE:</b> PEPF: – Physical Protection of Facilities – Every physical address point to facilities housing workstations that process of display sensitive information or unclassified information that has not been cleared for release is controlled during working hours and guarded or locked during non-work hours.					
In summary, all elements of a DoD information system IA program shall be deployed, implemented, and maintained through the DoD IA C&A process.					

2.2.2.3.2. Per AFI 31-501, *Personnel Security Program Management*, in order for foreign nationals to have access to any network and/or functional systems connected to those networks, they must have a favorable background investigation. The NAC must consist of: (a) host-government law enforcement and security agency records check at the city, state, province, and national level, (b) Defense Clearance and Investigation Index (DCII) check and (c) FBI check where information exist indicating residence by the foreign national in the United States for one year or more since the age of 18.

2.2.2.3.3. AFI 33-202, *Network and Computer Security*, states that Access by foreign nationals to Air Force information systems, networks and enclaves is not authorized unless approved by a lieutenant general or equivalent. This access was granted in AFSPC/CV letter dated 11 Oct 2001. Each wing may grant access to NIPRNet on an “as required” basis through the use of controls that limit the individual’s access to the network, after access to the local network has been approve

2.2.2.3.4. If foreign nationals require access to functional systems, the requesting organization must obtain approval by complying with Table 5.1 of AFI 33-202, such as; “HQ USAF 2-Letter Functional is the Approval Authority for access to that system”. 45 SW users requiring functional systems accessed such as Core Automated Maintenance Systems (CAMS) or Standard Base Supply System (SBSS) require approval for access from the respective functional manager. DISA Field Operations UNISYS Security Technical Implementation Guide, Version 4, Release 2, provides approval to foreign nationals to access these systems. It states that the security manager should place the Host Nation Agreement or Status of Forces Agreement number in block 10 of DD Form 2875.

### 2.3. How to Close An Account.

2.3.1. To close an account, the user or user’s supervisor should send a request to the Patrick Base C4 Helpdesk to have the user’s account disabled and subsequently deleted from the LAN on a specific date. The account will then be scheduled for deletion.

2.3.2. Accounts scheduled for deletion will be administratively disabled and hidden for 10 working days before final deletion occurs.

### 2.4. Modifying an Account.

2.4.1. Accounts need to be modified when one of the three following actions are necessary.

2.4.1.1. Separating from the organization of responsibility.

2.4.1.2. Change of organization (PCA).

2.4.1.3. Change of duty station (PCS).

2.4.1.4. Change of identity (marriage or divorce).

2.4.1.5. Who’s authorized to access an account when the user expires or is deceased.

2.4.1.6. Accounts that is inactive for 90 days or more.

### 2.5. The 45 SW ENTNet Minimum Information System Requirements.

2.5.1. Minimum system requirements exist, not to limit the types of systems connected to the ENTNet, but to ensure users have powerful enough equipment to utilize ENTNet services and standard software. Users with systems below the minimum specifications will suffer from poor performance (slow speed, software problems, inability to access the ENTNet or Internet effectively, etc.).

2.5.2. Systems connected to the ENTNet must comply with AFSPC standards from the Air Force Communications Agency’s website (<https://private.afca.af.mil/prodeval/Summary/std-top.htm>)

2.5.3. Users whose systems do not meet these requirements can have their units purchase new systems through the AFSPC approved process.

## 2.6. Standard ENTNet Software Provided to the User.

2.6.1. The 45th Space Wing will install, support, upgrade, and maintain the 45 SW ENTNet workstations. This includes, but is not limited to:

2.6.1.1. Air Force Space Command's (AFSPC) Approved Operating System.

2.6.1.2. CA Unicenter TNG Administration Tools.

2.6.1.3. SMS Administrative tools.

2.6.1.3.1. AFSPC Office Production Software, to include, but not limited to: MS Office Suite.

2.6.1.3.2. Adobe Acrobat Viewer.

2.6.1.3.3. Norton antivirus Software.

**NOTE:** Both of the AFSPC approved Antivirus and Form manipulation software are Department of Defense (DoD) licensed and DoD personnel (military and civil service) may install them on their home computer systems. Users must update their own anti-virus signature files on their home systems.

2.6.2. The 45 SW ENTNet organizational Information Technology personnel will regularly update standard software remotely. Software versions will not be upgraded on the product's immediate release, but only after AFSPC approval.

2.6.3. The above list of standard software is subject to continual change.

2.7. System Installs/Upgrades. Only authorized personnel are permitted to perform maintenance on the Enterprise Networked computers (e.g., no user should ever open the case of their PC). Call the Base C4 Help Desk System to open a help ticket to install/move systems, add cards, upgrade RAM, install/move printers, etc. This prevents users from causing unintended hardware damage to the network.

2.8. Passwords. All accounts on the ENTNet must utilize a secure passwords. Minimum requirements and guidance on creating passwords are included in paragraph [6.1](#).

## 2.9. Network/Mailbox Space.

2.9.1. Each user mailbox size will be based on space availability of the Enterprise Network.

2.9.2. Commanders and their deputies, executive officers, and Commander's personal assistants are automatically provided 200 megabytes of disk space on the Microsoft Exchange Storage Area Network (SAN) for Email; all others will be given a default of 50 megabytes.

2.9.3. The above list of disk space size limits is subject to continual change.

2.9.4. Users are encouraged to use their hard disk drives (C: and D: drives) to store information that does not need to be shared. Users are also responsible for backing up their information via a Zip disks, recordable CDs, and removable drives may be used to backup and/or transport large files between systems. Networked share drives are a community resource; do not store unnecessarily large files or multimedia (i.e., .wav, .gif, etc.) on them. SIPRNet users are encouraged to use the provided Network shares for mission critical files.

2.9.5. Email is easily stored and organized through MS Outlook. Directions for Email management are provided in AFI 33-119, *Air Force Messaging*, and paragraph 4.4., of this publication.

2.9.6. If additional network or mail server space is necessary, unit commanders or staff agency chiefs may submit a written request to the Base C4 Help Desk, 45 SCS/SCABC.

## 2.10. Modem Usage.

2.10.1. Use of dial-up modems is prohibited on any 45 SW ENTNet workstation unless specifically approved by the 45 SW ENTNet Designated Approving Authority (DAA). The Wing Commander (45 SW/CC) is the only DAA who can approve connections to the 45 SW ENTNet.

2.10.2. Modems will be removed or disabled from all workstations and laptops prior to being placed into operation on the 45 SW ENTNet. If your system comes with a modem installed, contact the Base C4 Help Desk (4-2666) to have it disabled or removed.

## 2.11. Telecommunications Monitoring and Assessment Program (TMAP).

2.11.1. The Air Force TMAP program monitors unsecured telecommunications systems to determine if these unsecured systems are used to transmit sensitive or classified information. Use of Air Force computer systems constitutes consent to monitoring and system testing. Each time a user accesses the ENTNet, he/she is required to give consent to monitoring by clicking the OK button at the bottom of the TMAP statement., as detailed below:

2.11.1.1. NOTICE AND CONSENT LOG-ON BANNER. "WARNING: This is a Department of Defense computer system. This computer system, including all related equipment, networks, and network devices (specifically including Internet access) are provided only for authorized U.S. Government use. DoD computer systems may be monitored for all lawful purposes, including that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability, and operational security. Monitoring includes active attacks by authorized DoD entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied, and used for authorized purposes. All information, including personal information, placed or sent over this system may be monitored. Use of this DoD computer system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal, or other adverse action. Use of this system constitutes consent to monitoring for these purposes. This site is intended for the use of the Air Force and DoD only. Do not reproduce or distribute the content of this site to a wider audience without coordination with the information owner and your unit public affairs office."

3. Training. The Base C4 Help Desk coordinates computer training for 45th Space Wing ENTNet users. A schedule of classes is located at <https://www.patrick.af.mil/45og/45scs/SCA/scab/training.htm>. . Class slots may be reserved by calling the Base C4 Help Desk at 494-6599, 4-6222 or 494-2666 or sending an e-mail request to "[sctraing@patrick.af.mil](mailto:sctraing@patrick.af.mil)"

## 4. Email.

### 4.1. Authorized Uses for Email.

4.1.1. The Air Force has published an instruction on using government Email systems, AFI 33-119, *Air Force Messaging*. This instruction is located on the Air Force publication web site and provides detailed information on rules, standards, and guidance relating to the proper use of Email by the Air Force. All new 45 SW personnel are also briefed on this information at the Base New-comers Orientation Briefing and by their respective ISSO.

4.1.2. Email may be used for two purposes--authorized or official business. Official business includes communications such as memorandums, orders, letters, or informal communications such as a replacement for telephone calls and notes. The user may also send informal communications to individuals. Authorized personal use includes brief communications made by DoD employees while traveling on US government business to notify family members of transportation or schedule changes. It also includes personal use such as checking in with spouse or minor children, scheduling appointments, or emailing directions to visiting relatives when the "agency designee" (the first supervisor who is a commissioned officer or a civilian above a GS -12) permits. Personal communication must not adversely affect the performance of official duties, must be of reasonable duration and frequency, and should be made, whenever possible, during the employee's personal time.

4.1.2.1. Unacceptable use of the 45th Space Wing Email system includes, but is not limited to:

4.1.2.1.1. Pornography, chain letters, jokes, unofficial advertising, soliciting or selling.

4.1.2.1.2. Inappropriately handled classified information.

4.1.2.1.3. Overburdening the email services with large files, especially when sending via broadcast or group mailing. A better solution is to place large files, (e.g. graphics files), on server and use links to these files versus overburdening the system with large data files, especially when sending via broadcasts or group mailings. Do not send un-official graphics files via the network, and use text messages whenever possible. Email messages sent off base or received from off base are limited to a size of 10 MB through Microsoft Exchange. For files that are larger than 10 MB Exceptions/workarounds can be worked on a case-by-case basis through the Base C4 Help Desk for users who have had their requirements validated.

4.1.2.1.4. Sending harassing, intimidating, abusive or offensive material to or about others violates Air Force standards. This includes junkmail, chain letters and any type of jokes or humor that is offensive or in poor taste. Email account users bear sole responsibility for material they send or access. Anyone receiving inappropriate or unauthorized Email should contact their Information Systems Security Officer (ISSO), the wing Information Assurance Office (45 SCS/SCBI), or the Base C4 Help Desk (4-2666).

4.1.2.1.5. Using another person's account or identity without proper authorization or permission.

## 4.2. Signature Blocks.

4.2.1. Organizational Email will contain a complete signature element clearly indicating who sent the message. Signature is indicated by the word "SIGNED" per AFI 33-119, Section C, paragraph 4.2.

**Table 2. Sample Signature Block.**

<p><b>- Military Signature Block</b></p> <p>//SIGNED//</p> <p>JOHN HANCOCK, 1st Lt, USAF</p> <p>Chief, Network Control Center</p> <p><b>- Civilian Signature Block</b></p> <p>//SIGNED//</p> <p>Char Broil, GS-12, DAF</p> <p>Branch Chief, Field Support</p> <p><b>- Contractor Signature Block</b></p> <p>//SIGNED//</p> <p>John, DOE, Contractor, 45 SCA/CSR</p>
---

4.2.2. Individual Email messages should identify the sender and their phone number, but can use a less formal signature element. Graphics to include non-standard background should not be attached to signature blocks, due to the unnecessary size increase which they add to the email.

4.3. E-STAFFING. The process currently being used to accomplish official coordination as directed by AFSPC is by using a Microsoft Exchange form (.OFT) labeled E-Staffing, which is located in the public folders of the 45SW Exchange Server. However, as of this writing, AFSPC is in the process of converting all AFSPC units over to a Pure Edge form sent via exchange. AFSPC will provide training and written guidance on E-Staffing utilizing the Pure Edge form process, in the near future. Once available, this guidance will take precedence over this paragraph.

#### 4.4. Email Management.

4.4.1. Email is used more and more for everyday official communications, notifications, and announcements. Although it is important to save Email for record keeping purposes (see AFI 33-119, paragraph 8), we must balance this with the space available on the Enterprise networks.

4.4.2. Email left in your ENTNet mailbox takes up space on network servers. When you reach a storage limit (see paragraph 2.7.) you will receive an error message stating that the disk or your mailbox is full. NOTE: Mail items in your MS Outlook "Deleted Items" and "Sent Items" folder count towards your quota. To free the space used by the "Deleted Items" folder, select *Empty "Deleted Items" folder* in MS Outlook's *Tools* menu or copy them to a personal folder.

4.4.3. Email you wish to keep should be stored and organized in a MS Outlook personal folder (which moves your messages from the network to your local hard drive or another storage media). Messages can be transferred by "dragging and dropping" them into a personal folder. Assistance is available in moving messages into personal folder in the MS Outlook *Help* menu. Remember, Backing up of information which resides on your computer is your responsibility, so please perform your backup of machine as much as possible.

4.5. Forwarding Official E-Mail. Official Email traffic is prohibited from being auto-forwarded to commercial Email accounts or from being transmitted through civilian Email providers; this includes

the use of personal Email accounts. Customers may manually forward Email, “message-by-message” to commercial accounts after ensuring that all information in the message is unclassified and that it does not contain information that is not authorized for release to the public.

4.6. Commercial Email Services. Personnel shall not use commercial Email accounts in place of their 45 SW email account. Access to Internet service/email providers, such as *America Online*, *CompuServe*, *Hotmail*, *Yahoo Mail*, or others through the 45 SW LAN, is prohibited (i.e., users shall not use 45 SW Enterprise to check personal Email accounts). Users are provided government email accounts to use for authorized or official purposes, all others should not be performed from the 45 SW Enterprise.

4.7. Global Email Distributions.

4.7.1. Global Email. ENTNet wide Global Email (email to all LAN users) usage is reserved for critical, time-sensitive information of interest to the entire base populous (i.e., changes in FPCON/INFOCON, service outages, security notices, etc.). Requests for global Email distribution shall be staffed through unit commanders to the Base C4 Help Desk (45 SCS/SCABC).

4.7.2. Organizational ‘Global’ Email. The Base C4 Help Desk is also the focal point for Email distribution of non-critical information of interest to the entire base populous (i.e., office hour changes, special events, etc.). These messages are forwarded to a single point of contact (usually the unit’s organizational account) in each ENTNet connected organization. These individuals then forward the message, through their own chain of command procedures, to their entire organization.

4.7.3. If you wish to disseminate information via the Email system, to a group or user, do not hesitate to contact the Base C4 Help Desk at 494-2666. These individuals will be happy to discuss with you the proper procedure for disseminating your information to the appropriate people.

4.8. Remote Access. See paragraph 5.3. for instructions on connecting to your ENTNet account from off base, which will allow you to remotely connect and check you official email.

5. Use of the ENTNet and the Internet.

5.1. Appropriate Use.

5.1.1. Accessing the ENTNet or Internet through a government computer or network involves use of a government resource. The ENTNet and the Internet provides opportunities for quick and efficient disseminating of information to the base populous and 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 World Wide Web (WWW). The Air Force networks and Internet goal is to provide maximum availability at an acceptable risk level for users needing access for the execution of authorized or official business. Government-provided hardware and software is for conducting official and authorized government business only. Using the Internet for other than authorized purposes may result in adverse administrative or disciplinary action.

5.1.2. Unauthorized use of government computer systems and the Internet is punishable under DoD 5500.7-R (Joint Ethics Regulation) chapter 2 (incorporating by reference 5 CFR 2635.704), AFI 33-119, AFI 33-129, and any other applicable AFI.

5.1.3. The following activities involving the use of ENTNet computer hardware or software are specifically prohibited:

5.1.3.1. Storing or processing classified information on any system not approved for classified processing.

5.1.3.2. Any use of government-provided computer hardware or software for other than authorized or official government business.

5.1.3.3. Any use for personal or commercial financial gain. This includes, but is not limited to, chain letters, commercial solicitation, and sales of personal property (excluding authorized communications to the base bulletin).

5.1.3.4. 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 (i.e., swastikas, neo-Nazi materials, etc.), and sexually harassing materials. Obscene material includes, but is not limited to, pornography and other sexually explicit materials.

5.1.3.5. Storing or processing copyrighted material (including cartoons) unless approval is obtained from the author or publisher.

5.1.3.6. Using Instant Messenger or Buddy List services such as *ICQ*, *AOL Instant Messenger (AIM)*, or *Yahoo Instant Messenger*.

5.1.3.7. Participating in "chat rooms" or open forum discussion unless for official purposes and after approval by appropriate Public Affairs channels.

5.1.3.8. Using another person's account or identity without appropriate authorization or permission.

5.1.3.9. Viewing, changing, damaging, deleting, or blocking access to another user's files or communications without appropriate authorization or permission.

5.1.3.10. Attempting to circumvent or defeat security or auditing systems without prior authorization or permission (such as for legitimate system testing or security research).

5.1.3.11. Obtaining, installing, copying, storing, or using software in violation of the appropriate vendor's license agreement.

5.1.3.12. Installing or using non-approved software or games (commercial, freeware, or otherwise). All software purchases must follow procedures in paragraph 7. of this instruction.

5.1.3.13. Use of streaming audio/video (i.e., *RealAudio* or *Windows Media Player Streaming Audio*) from sites outside of the *.mil* or *.gov* domains.

5.1.3.14. Permitting an unauthorized individual access to a government-owned or government-operated system.

5.1.3.15. Modifying or altering the network operating system or system configuration without first obtaining permission from the administrator of that system.

5.1.4. Unit commanders may authorize personnel, in writing, use of government resources to further their training or professional, military or academic knowledge, if they determine it is in the best interest of the government.

5.2. Commercial Internet Access. Users may not connect to commercial Internet Service Providers (ISPs), such as *America Online*, *CompuServe*, *Earthlink*, or other ISPs from systems connected to the ENTNet or systems that can connect to the Enterprise Network (i.e., ENTNet laptops).

5.3. Remote Access. The Network Control Center (NCC) maintains servers to allow remote (dial-in) access to the base Enterprise Network Email systems. For security reasons, these servers are the only authorized dial-in equipment for remotely accessing base network services.

## 6. Security.

### 6.1. Passwords.

6.1.1. Passwords must contain at least eight alphanumeric characters, must contain upper and lower case characters, at least one number, and at least one special character, and may not utilize any 4 character's of a dictionary word, or substitute characters, such as an zero ("0") for an alpha "O".

6.1.1.1. English upper case alphabet (A, B, C ... Z).

6.1.1.2. English lower case alphabet (a, b, c ... z).

6.1.1.3. Numerals (0, 1, 2 ... 9).

6.1.1.4. 'Special characters' ([ ] { } ; := + - \_ ) \* & ^ % \$ # @ ! ~ ` / ? . > , < \ | ).

6.1.2. Passwords should be easy to remember but hard to guess. Be creative by taking a phrase that is easy to remember. Use the first letter of each word, and add any appropriate capitalization, punctuation, and other character manipulations. For example, "three blind mice, see how they run" would be 3Bm\$\$shtr.

6.1.3. Do not construct passwords that could be related to your personal identity, family members, pets, home or work environment.

6.1.4. Do not use dictionary words of any language or commonly known phrases. Numeric values and special characters should be embedded within the password and not used at the beginning or at the end.

6.1.5. Passwords must be updated every 90 days, to ensure the security of our system. You will be reminded by the system 14 days before your current password expires.

6.1.6. Passwords are the gateway to our network. Do not give out your password to anyone. Remember that the Enterprise administrators will never call asking for your password.

6.1.7. All passwords are checked for compliance with the Enterprise policy before being accepted during the password change. The AFSPC Network Operation and Security Center (AFSPC NOSC) will routinely attempt to 'crack' or 'break' system passwords to ensure network security. Any password that is cracked will be required to be changed immediately.

### 6.2. Antivirus.

6.2.1. The threat of a virus on the network and the damage that can occur is a major security concern. To protect against this threat, the Enterprise has adopted the use of Air Force standard anti-virus software.

6.2.2. All workstation computers connecting to the ENTNet must have the approved AFSPC anti-virus loaded on it. The ENTNet administrators will automatically update anti-virus detection signatures files. If a system is noted as not having an anti-virus software loaded or if the anti-virus software on it, please notify the Base C4 Helpdesk.

6.2.3. Do not interfere with or prevent the Antivirus software from running; this defeats the purpose of having the software. However, users may continue to use their workstations with the anti-virus software running in the background.

6.2.4. Users must immediately report all viruses detected on their workstations to the Base C4 Help Desk (4-2666) and notify their Information Systems Security Officer (ISSO). The ISSO will then forward virus reports to both the Wing Information Assurance Office (45 SCS/SCBI), and Network Control Center (NCC) (45 SCS/SCABA).

### 6.3. Screen Savers.

6.3.1. The first line of defense for the security of the Enterprise is the individual user. All users are responsible for the actions originating from their personal accounts. Leaving an unattended terminal (PC) logged on to the LAN is a common and very unsecured practice.

6.3.2. A password protected screen saver is the best countermeasure to ensure the security of the 45 SW ENTNet and the security of the individual's account. The Patrick-2k domain administrators will implement a 10 minute time as directed by the Network Control Center (NCC). No individual is authorized to disable this, without explicit permission from the NCC.

6.3.3. For increased security, all users will manually lock their workstations whenever leaving their system unattended and/or out of sight of view. You may do this by holding the *Ctrl* and *Alt* buttons on the keyboard and pressing *Delete*; then select *Lock Workstation* with the mouse from the displayed menu. For further assistance, contact the Base C4 Help Desk (4-2666).

### 6.4. INFOCON.

6.4.1. In May 1999, the Secretary of Defense established INFOCONs (or Information Operations Conditions) to recommend "actions to uniformly heighten or reduce defense posture, to defend against computer network attacks, and to mitigate sustained damage to the DoD information infrastructure, including computer and telecommunications networks and systems."

6.4.2. INFOCONs are much like the FPCONs we use to indicate the current force protection threats we are facing; except INFOCONs assess the threat of information/electronic warfare.

6.4.3. Similar to FPCONs, INFOCONs are represented by 5 levels:

6.4.3.1. INFOCON Normal – No significant activity.

6.4.3.2. INFOCON Alpha – An increased risk of information attack.

6.4.3.3. INFOCON Bravo – A specific risk of information attack.

6.4.3.4. INFOCON Charlie – Limited information attacks in progress.

6.4.3.5. INFOCON Delta – General information attacks in progress.

6.4.4. Like FPCONs, certain tasks must be performed to attain each INFOCON level. For INFOCONs, most actions are completed by the Network Control Center (NCC), Enterprise administrators, the Wing Information Assurance Office (IAO), and unit ISSOs. Users, however, are our first

line of defense against information attacks. Users must immediately report any suspicious events (unknown individuals trying to access your computer, possible computer viruses, phone calls asking for your password, etc.), at any INFOCON level, to your unit ISSO and the Base C4 Help Desk (494-2666).

#### 6.5. AFCERT Direction.

6.5.1. The mission of the Air Force Computer Emergency Response Team (AFCERT) is to provide information assurance assistance to Air Force units. The AFCERT conducts operations involving computer intrusion detection, incident response, computer security information assistance, and vulnerability assessment of Air Force computer systems. At the base level, AFCERT direction and guidance is disseminated through regular command channels, the Network Control Center, the IAO or the formulate local CERT.

6.5.2. At times, it is necessary to quickly implement changes to the ENTNet to ensure our continued security. Any actions users must take will be directed through the chain of command, the Base C4 Help Desk, or by the unit's ISSO(s).

#### 7. Process Workflow Requirement Resource (PWRR).

7.1. Units wishing to purchase new computer systems, computer equipment (i.e., printers, memory, disk drives, etc.) or 'non standard' computer software must document their requirement (e.g., what purposes they intended to use the system for) using PWRR Manager. PWRR Manager is the command's official tool used to initiate, maintain, and track the lifecycle progress of requirements. It replaces the AF Form 3215, *IT/NSS Requirements Document*. The organization (user) requesting C4 equipment, services, or systems will identify their mission need by submitting a requirement on the web-based PWRR system located at <https://pwrr.afspc.af.mil>.

7.2. The requirement will be automatically routed to the appropriate office for validation. C4 capabilities cannot be purchased unless an approved requirement has been submitted and a valid technical solution has been developed.

MARK H. OWEN, Colonel, USAF  
45 SW Commander