



DEPARTMENT OF THE AIR FORCE

HEADQUARTERS UNITED STATES AIR FORCE ACADEMY

USAF ACADEMY, COLORADO

USAFAI33-118_USAFAGM2016-01

9 September 2016

MEMORANDUM FOR USAFA ALL

FROM: USAFA/CC

SUBJECT: United States Air Force Academy (USAFA) Guidance Memorandum (GM) to USAFA Instruction 33-118

1. By Order of the Superintendent, this Guidance Memorandum implements changes to USAFA Instruction 33-118, *USAFA INFORMATION TECHNOLOGY ENTERPRISE USE AND MANAGEMENT*, effective 15 September 2016. These changes add further restrictions to the use of USAFA educational and mission networks. Compliance with this memorandum is mandatory. To the extent its direction is inconsistent with other USAFA publications, the information herein prevails, in accordance with AFI 33-360, *Publications and Forms Management*.
2. Paragraph 14, Inappropriate Use of Computers on USAFA Networks, is modified to include restricting streaming video on USAFA educational or mission networks. The NIPRNet, USAFA.EDU, ResearchNet, and other government funded commercial networks will not be utilized for streaming video (e.g., Netflix, Hulu, HBOGO) for non-mission or non-educational purposes. The 10th Air Base Wing (ABW) will acquire and utilize tools to implement and enforce this policy. The 10 ABW will also develop processes and procedures to enable the use of streaming video for legitimate mission-related purposes on the USAFA.EDU network.
3. Paragraph 21, Port Exceptions, is changed to ensure compliance with the DoD Ports, Protocols, and Services Management (PPSM). This Guidance Memorandum rescinds all port exceptions previously approved for the USAFA.EDU network for the purposes of morale, welfare or recreational purposes. The DoD PPSM Registry Database is the only authoritative source for Ports, Protocols, and Services information. The USAFA.EDU Authorizing Official must approve any requests to open ports not approved in the PPSM Registry Database.
4. This memorandum becomes void after one year has elapsed from the date of this memorandum or upon publication of an Interim Change or a rewrite of the affected publication, whichever is earlier.

MICHELLE D. JOHNSON
Lieutenant General, USAF
Superintendent

**BY ORDER OF THE
SUPERINTENDENT**

**HQ UNITED STATES AIR FORCE
ACADEMY INSTRUCTION 33-118**

6 MARCH 2013



Communications and Information

**USAFA INFORMATION TECHNOLOGY
ENTERPRISE USE AND MANAGEMENT**

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available for downloading or ordering on the e-Publishing website at www.e-publishing.af.mil.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: HQ USAFA/A6I

Certified by: HQ USAFA/A6
(Lt Col Gary Denney)

Pages: 20

This instruction implements Air Force Policy Directive (AFPD) 33-1, *Cyberspace Support*. The purpose of this publication is to provide guidance for the use and management of Enterprise Information Technology (IT) Systems on the United States Air Force Academy (USAFA). It includes USAFA policy for client systems management, software, peripheral management, removable media, public web site, social media, Knowledge Management, acceptable use, network management, access management and account management. Guidance for IT Enterprise Use and Management is addressed in several Federal, Department of Defense (DoD) and Air Force publications (see Attachment 1). All USAFA organizations and personnel will comply with this higher-level guidance unless exceptions or waivers are requested and approved as specified in this instruction. This instruction applies to all USAFA personnel. It does not apply to Air Force Reserve Command units or the Air National Guard. Refer recommended changes and questions about this publication to the Office of Primary Responsibility using Air Force (AF) Form 847, *Recommendation for Change of Publication*. Ensure all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of in accordance with the Air Force Records Information Management System (AFRIMS) Records Disposition Schedule located at <https://www.my.af.mil/afirms/afirms/afirms/rims.cfm>. The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the Air Force. See Attachment 1 for a glossary of references and supporting information.

2.	Contractor Owned Computers.	3
3.	Hardware and Software Baselines.	3
4.	Software Approval.	4
5.	Removable Storage Devices and Media.	4
6.	Public Web Site Policy.	5
7.	Personally Identifiable Information (PII) Policy.	5
8.	Admissions Public Key Infrastructure (PKI) Policy.	6
9.	Electronic Messaging.	6
10.	Electronic Mail Mass Distribution (Distro) Lists.	6
11.	IT Acquisitions.	7
12.	Digital Printing and Imaging (DPI) Consolidation.	8
13.	.EDU Network Account Authorization.	8
14.	Inappropriate Use of Computers on USAFA Networks.	9
15.	CAC Removal Lock Policy.	10
16.	User ID and Password Access for Administrator Accounts.	11
17.	IA Certification Requirements.	11
18.	Guest Accounts for	12
19.	Global Address List (GAL) Title Field.	12
20.	Internet Blocking.	12
21.	Port Exceptions.	13
22.	Inactive LAN Drops (Switchports).	13
23.	BlackBerry, Personal Data Assistant (PDA) and Cell Phone Authorization.	13
24.	Television Services.	14
25.	Video Teleconference (VTC).	14
26.	Internet Service Requirements.	15
Attachment 1—GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION		16
Attachment 2—COTS SOFTWARE APPROVAL PROCESS		19
Attachment 3—REQUIREMENTS FOR COMMERCIAL ISP LETTER		20

1. Privately Owned Devices on . EDU.

1.1. The following actions are required to mitigate risk associated with this exception to AFMAN 33-152, *User Responsibilities and Guidance for Information Systems*, Paragraph 2.12, which states, “using privately-owned hardware and software for government work is

strongly discouraged; however, it may be used for processing unclassified and sensitive information with justification and Designated Accrediting Authority (DAA) approval”:

1.1.1. Only properly configured cadet/government-owned computers are authorized for use on the .EDU domain.

1.1.2. While at USAFA, Cadets will not connect their computers to the .EDU network while simultaneously using modems or wireless cards to access another network (i.e. Verizon, AT&T, Sprint Broadband cards).

1.1.3. All privately-owned Cadet computers are subject to government monitoring and will be made accessible to security vulnerability scans.

1.1.4. Security vulnerability scans shall be conducted on Cadet issued computers when introduced to the USAFA enclave as established in USAFAI 33-119, *Information Technology Service Operations Management*.

1.2. Requests for other privately owned devices connecting to government owned equipment on the .EDU network must be approved In Accordance With (IAW) USAFAI 33-116, *Information Technology Change Management*, paragraph 3.

1.3. IAW DoD Chief Information Officer memo, *Use of Commercial Mobile Devices Not Connected to DoD Networks*, dated 31 July 2012, “Processing, storing, transmitting, or receiving any FOUO or non-publicly releasable data is not authorized.” Mobile devices that are on the DoD Unified Capabilities Approved Products List are approved for purchase, but are not authorized for connection to any DoD-owned or DoD-funded network. All exceptions must be requested via Work Order Management System (WOMS) and will be processed for waiver approval by the DAA.

2. Contractor Owned Computers. To meet USAFA mission requirements, some contractors are authorized by 10th Communications Squadron (10 CS) to connect corporate computers to the .EDU network to perform government assigned official business IAW AFI 33-112, *Information Technology Hardware Asset Management*, paragraph 13.

2.1. All contractor-owned devices must comply with USAFA, AF and DoD computer information security requirements and directives. The devices are subject to government monitoring and will be made accessible to security vulnerability scans.

2.1.1. Security vulnerability scans will be conducted by 10 CS prior to connecting to the USAFA enclave and subject to monitoring based on policies established in USAFAI 33-119.

2.2. Requests to connect contractor-owned computers must provide justification and duration, and be approved IAW USAFAI 33-116, paragraph 3.

3. Hardware and Software Baselines. The 10 CS is responsible for creating and maintaining the official .EDU IT baseline. The Director of Academic Computing is responsible for creating and maintaining the approved .EDU IT baseline additions. Any deviations from the official .EDU IT baseline will be approved by the Change Advisory Board (CAB) IAW USAFAI 33-115, *Information Technology Service Configuration Management*, and USAFAI 33-116 and AFI 33-210, *Air Force Certification & Accreditation (C&A) Program (AFCAP)*. Only baseline images and configurations approved by the CAB will be allowed for use on the .EDU network.

4. Software Approval. To meet the USAFA academic requirements and the athletic mission, a streamlined process is necessary to allow the USAFA DAA to assess the risk of adding Commercial-Off-The-Shelf (COTS) software, to include Freeware and Shareware for the purpose of meeting the academic mission, for the ResearchNet and .EDU networks, reference Attachment 2 and USAFAI 33-116, paragraph 3. Each WOMS software request will include a completed USAFA Form 136, *Software Approval Questionnaire*, as an attachment with the WOMS request. Freeware and Shareware are authorized but will be virus checked by the user prior to use, and will be registered via the 10 CS IT Services Catalog (<https://eis.usafa.edu/centers/it/SitePages/ApprovedSoftware.aspx>).

4.1. If it is discovered through the USAFA Software approval process that a network vulnerability has occurred, the enclave administrator (10 CS, ResearchNet Client Systems Technicians (CST)) will take actions to mitigate the risks. If a critical risk cannot be mitigated the software will be removed immediately by the responsible CST.

4.2. USAFA academic exercises that require cadets, faculty and staff to develop software for non-operational usage are exempt from these software approval requirements. Software solutions that support any USAFA operations will be submitted to the CAB IAW USAFAI 33-116. If a Cadet developed software application is discovered to cause a network vulnerability, 10 CS will remove immediately.

5. Removable Storage Devices and Media. Removable storage devices and media used on USAFA networks will comply with requirements in AF DAA “Combined Implementation Guidance for USCYBERCOM CTO 10-084 and 10-133,” dated 6 Jul 2011, and Air Force Network Operations Center, NETOPS Tasking Order 2008-323-001, unless expressly exempted below:

5.1. Only government-procured removable media and storage devices may be used in government-furnished computer systems connected to any ResearchNet and .EDU network at USAFA. Cadets may use non-government procured, external removable non-flash media devices with their officially approved personally owned computers for academic and research purposes. Cadet candidates may use non-government procured, external removable non-flash media devices with their government purchased computers. Instructors are allowed to connect cadet personally owned devices to government computers for academic and research purposes only. All personnel must ensure that they are running anti-virus software with current antivirus signatures from 10 CS, and must scan all removable media prior to use. Requests for other privately-owned, non-flash media devices connecting to officially-approved, personally-owned computers on the .EDU network must be approved IAW the WOMS process.

5.2. Only USB/Flash media drives that meet the following requirements are authorized on the .EDU network:

5.2.1. Must be Data-at-Rest compliant using onboard hardware based encryption.

5.2.2. Must have firmware that is digitally signed and verified.

5.2.3. Must be Federal Information Processing Standard 140-2 certified, exception to policy letter and must be on file with Wing Information Assurance Manager.

5.2.4. Device must be listed on the Data-at-Rest bulk purchase agreement and have an AFVA 33-276, *Air Force Privacy Act Label*, attached.

5.3. All personnel must scan removable media, with anti-virus software running current signatures, prior to connecting to any USAFA network.

5.4. Use of any removable storage device or media that does not meet the above specifications is not authorized for use on any computer connected to a USAFA network and is subject to confiscation.

6. Public Web Site Policy. For .EDU, USAFA/Public Affairs (PA) must approve all USAFA public facing websites. USAFA Mission Partners (MP) and units must submit the following information to USAFA/PA for any public facing websites (including .EDU, .MIL, .Org, .Com, .Net, etc.) associated with their organization:

6.1. Documentation of MP Director or Unit Commander/Director approval for the website.

6.2. Justification for the website.

6.3. Source of funding for the website.

6.4. Name and contact information for the website maintainer.

6.5. With the exception of enterprise event hosting, no AF OPSEC Critical Information List items will be posted on a public facing website.

7. Personally Identifiable Information (PII) Policy. For non-authenticated Public Web Pages, IAW AFI 33-129, *Web Management and Internet Use*, paragraph 6.5.1, to accomplish the education and research mission, USAFA faculty departments may include some PII on their approved public facing websites in order to help foster collaborative work with other colleges and universities.

7.1. Requests to place PII on USAFA public facing websites must be approved IAW USAFAI 33-116, paragraph 3.

7.2. Each individual person must authorize, in writing, for their PII to be included on any public facing web sites.

7.3. SSNs, birthdates, home address, personal phone numbers and spouse/dependent information are not allowed on public web pages under any circumstances.

7.4. The following USAFA faculty information is allowed on approved USAFA public websites:

7.4.1. Instructor names and instructor photos.

7.4.2. Instructor contact information (office address, phone, and e-mail).

7.4.3. Instructor education (schools and degrees – academic, not Professional Military Education).

7.4.4. Instructor research interests and professional biographies.

7.4.5. Instructor publication lists, links to instructor research products/software in the public interest.

8. Admissions Public Key Infrastructure (PKI) Policy. The Admissions authenticated public facing websites (i.e. <https://admissions.usafa.edu>) does not require PKI client certification via Common Access Card (CAC). Although DoDI 8500.2, *Information Assurance (IA) Implementation*, Mission Assurance Category III Controls requires “Identification and authentication to be accomplished using the DoD PKI Class 3 certificate and hardware security token (when available),” USAFA has a mission requirement to allow external users to access and use the Admissions public facing web site. Most users of this site do not have CACs and DoD certs are not recognized by the certification authorities accessed by today's web browsers. To mitigate risks associated with this exception, the following actions are required:

8.1. The USAFA Admissions public facing website will use Commercial Secure Socket Layer (SSL) server certificates instead of DoD SSL Certificates.

8.2. USAFA Admissions will implement user ID/password login for sites that require authentication. Passwords must meet the minimum requirements of Defense Information Systems Agency (DISA) Access Control Security Technical Implementation Guide (STIG), AFMAN 33-282, *Computer Security (COMPUSEC)*, paragraph 4.5.

8.3. USAFA Admissions is required to comply with AFI 33-332, *Air Force Privacy Program*, Chapter 2, *Collecting Personal information from Individuals*.

8.4. All users of the Admissions public facing web site (except applicants) must complete IA Awareness Training.

9. Electronic Messaging. USAFA personnel will follow guidance in AFMAN 33-152, section 6 regarding electronic messaging policy. Requests for exceptions to electronic messaging policy must be approved IAW USAFAI 33-116, paragraph 3. Users should minimize the use of images or attachments by using hyperlinks in order to save bandwidth and email box sizes.

9.1. Users creating an out-of-office email/voicemail must refrain from using: Exact deployment/leave/TDY dates, deployment/leave/TDY locations, description/nature of absence, or any personal details that might lead to exploitation.

9.2. An example of a properly formatted out-of-office e-mail/voicemail reply is as follows: “I’m currently out of the office. In case of an emergency please contact me on my cell phone at XXX-XXXX. For routine program inquiries please contact Lt Dziokonski at XXX-XXXX and for all other branch requests please contact Lt Gilmore at XXX-XXXX.”

10. Electronic Mail Mass Distribution (Distro) Lists. The following policy is mandatory for all USAFA personnel when sending information to USAFA e-mail mass distro lists:

10.1. IAW AFI 33-332, do not send any PII information to a mass distro list unless each member has an official need to know the personal information.

10.2. The first line of every e-mail using mass distro lists must include an approval statement (i.e., THIS DISTRIBUTION (A, O, P or USAFA_ALL MESSAGE APPROVED BY (name of commander, department head or director)).

10.3. Mass distro list descriptions/requirements:

10.3.1. Distro A: Only commanders, department heads, directors or their designated representative (in writing) may use this list which, goes to all 2-letter and tenant

organization mailboxes. Use this list for the direct attention of commanders, directors and department heads. Encrypted emails are authorized for use with this distro list.

10.3.2. Distro O: Only commanders, department heads, directors or their designated representative (in writing) may use this list. This list goes to all organization mailboxes for distribution by mailbox monitors to appropriate persons within the organization. When using this distribution, the line after the approval statement describes the target group for the message (e.g., PLEASE DISSEMINATE TO ALL RECORDS CUSTODIANS). Mailbox monitors will forward the message appropriately. Encrypted emails are authorized for use with this distro list.

10.3.3. Distro P_EDU: This list goes to all USAFA personnel except cadets and cadet candidates. The Superintendent, Commandant, Dean of Faculty, 10th Air Base Wing Commander, Preparatory School Commander and Director of Athletics and their designated representatives (in writing) are the approval authorities for this distribution. Use it only for time-sensitive, urgent and official business that requires the immediate attention of the vast majority of recipients. Unauthorized use includes any retirement invite, office party, going away, fundraiser, encrypted email, etc.

10.3.4. USAFA_All: This list goes to every network user, including cadets and cadet candidates. The Superintendent, Commandant, Dean of Faculty, 10th Air Base Wing Commander, Preparatory School Commander and Director of Athletics and their designated representatives (in writing) are the approval authorities for this distribution. Use it only for time-sensitive, urgent and official business impacting all personnel; i.e., notices of road closures, weather-related restrictions or closures, impending disaster, or other topics of similar gravity. Encrypted emails are unauthorized for use.

11. IT Acquisitions. All USAFA acquisitions (e.g., services, computers, peripherals, network devices, etc.), excluding Research funded acquisitions, must be approved IAW USAFAI 33-101, *Information Technology Service Strategy and Governance*, paragraph 3 or IAW IT Financial Working Group (ITFWG) processes. The USAFA/A6 will consolidate all IT Enterprise requirements and advocate for funding (via the ITFWG and USAFA/FM's financial processes). If funds are not available to procure the approved item(s), the requesting units may choose to use unit funds to procure the item(s) or wait until the funds are made available to the ITFWG. All IT hardware purchases must be procured using the approved Air Force Way process IAW AFMAN 33-152, paragraph 2.8. All IT acquisitions made outside of these processes must have a waiver from 10th Contracting squadron. All government owned (either centrally purchased or unit funded), contractor owned or privately owned will be Energy-Star rated and optimized to use the least amount of energy necessary to perform its function.

11.1. All USAFA IT acquisition requests must address planning for Lifecycle Replacement (LCR). Depending on resource availability, the following are LCR standards for USAFA assets:

11.1.1. Desktops – 5 years.

11.1.2. Laptops – 4 years.

11.1.3. Monitors – until no longer functional.

11.1.4. Servers – 5 years (as virtualized computing infrastructure is implemented, servers will be kept until no longer functional).

11.1.5. Printers/Multifunctional devices – until no longer functional or cost effective.

11.1.6. Switches/Routers – 5 years.

12. Digital Printing and Imaging (DPI) Consolidation.

12.1. The 10 CS will ensure all DPI purchases are made IAW USAFAI 33-119 and USAFA IT Acquisition Policy and will strive to have a minimum of a 12:1 ratio.

12.2. If the requested DPI is not included in the USAFA IT Service Catalog, the request must be approved by the CAB IAW USAFAI 33-116, paragraph 3.

12.3. USAFA will also make every effort to redistribute DPI to the maximum extent possible. Operational DPI that is no longer necessary will be turned in IAW AFI 33-112, for re-utilization across USAFA. These devices will be considered for re-use prior to purchase of new devices.

12.4. Each unit will procure or lease copier/fax/all-in-one office devices through individual Defense Logistics Agency Document Services contract or purchase only approved printers.

13. .EDU Network Account Authorization. The .EDU network was established to support the academic mission.

13.1. The following are authorized to have .EDU network user accounts:

13.1.1. All Cadets and personnel in Direct Reporting Unit (DRU) A-Staff, Dean of Faculty (USAFA/DF), Commandant of Cadets (USAFA/CW), Athletics (USAFA/AD), Admissions (HQ USAFA/RR), the Preparatory School (USAFA/PL), the Base Library (FSDL), the Cadet Administrative Management Information System Program Management Office, and .MIL SharePoint users (for SharePoint use only).

13.1.2. All other personnel will only be authorized .EDU network user accounts if their mission and interaction with the academic mission or personnel justifies an account. Personnel that currently have .EDU network accounts are authorized to retain their accounts, but are subject to revalidation. During revalidation, if the account is not required 10 CS is authorized to terminate the account. Interim system access may be granted for less than 1 duty day if system access is required to complete electronic versions of DD Form 2875 and/or AF Form 4394, per AFMAN 33-152, paragraph 2.3.6.

13.2. Access to the .EDU network is limited to the organizations listed above; requests from outside these organizations must be submitted IAW USAFAI 33-116, paragraph 3 and approved by the CAB. Justification for .EDU accounts for other personnel should include mission and academic interaction with cadets and USAFA/DF, USAFA/CW, USAFA/AD, HQ USAFA/RR and USAFA/PL faculty. Requests should also include level of account/access required: access to core services only (e.g., SharePoint, Cadet Administrative Management Information System, etc.), access to .EDU e-mail account only, or full network user access (i.e., core services, e-mail, access to internet, access to network resources, Virtual Private Network (VPN), etc.).

13.3. All .EDU network users are accountable for their on-line activity and are required to sign a Network Users License Agreement (NULA) while using the network.

13.4. All .EDU network users are authorized to use VPN to access the .EDU network when outside the domain.

13.5. All .EDU network users are required to run antivirus software and to scan all downloaded and installed files to help prevent damage to the .EDU network and its information/data.

13.6. .EDU accounts will be disabled after 30 days of inactivity unless extended absence is identified to the 10 CS IT Service Desk in advance (e.g., Deployment, Temporary Duty, etc.).

13.7. Cadet/Cadet Candidates accounts will be disabled by the 10 CS within 5 duty days after graduation and deleted after 30 days.

13.8. Visiting faculty and staff are authorized access to the academic enclave for official government purposes. The visiting member and their government sponsor should contact 10 CS IT Service Desk to receive an account.

14. Inappropriate Use of Computers on USAFA Networks. Personnel will not use the network to interfere with system security or integrity, obstruct users from authorized services, or conduct harassing activities toward other network users. User conduct that is inconsistent with IA policies and guidelines may result in immediate suspension of access to unclassified and classified Information Systems regardless of security clearance (NAC, Secret, Top Secret); Reference AFMAN 33-152, paragraph 3.2. Prohibited activities include but are not limited to the following:

14.1. Transmitting, displaying, or storing offensive, discriminatory, pornographic, inappropriate sexually related material, or accessing any web site that contains pornographic material.

14.2. Unauthorized sharing of copyrighted intellectual property (e.g., software, video, music). The .EDU network will not be used for sharing or distribution of copyrighted software or material unless the copyright specifically grants free and unrestricted distribution or authorized by the owner of the copyright. This includes but is not limited to network shared drives, file shares or file sharing sites on the internet (e.g., RapidShare, FileHippo, BearShare, KeepandShare, etc). Consult the Staff Judge Advocate for a determination on whether a proposed use, taking, and/or copying of intellectual property is permissible.

14.3. Breaking into any device, improperly accessing data files and/or hacking programs without permission in writing by the functional system owner.

14.4. Releasing a virus or a program that negatively impacts a system and/or hinders other computing devices.

14.5. Exploiting security gaps or efforts to circumvent present security measures. (e.g., anonymizer, port filters, p2p clients, etc.).

14.6. Hindering supervisory, maintenance, or accounting functions of the systems. (e.g., disabling or hindering Antivirus, SCCM, alerting/deleting system logs/files, etc.).

14.7. Tapping phone or network lines.

14.8. Establishing any non-approved remote access and connections to servers or personal computers on the .EDU network without authorization.

- 14.9. Monopolizing computer resources or computer access.
- 14.10. Obtaining, possessing, using, or attempting to use someone else's user account or password.
- 14.11. Accessing, or attempting to access, another user's data or information without proper authorization.
- 14.12. Sending junk mail, chain letters, ghost writing email, using email resources to disrupt or overload mail services within or outside USAFA via "email bombing" or "spamming."
- 14.13. Using government computing resources to engage in ethnic, racial, or sexual harassment of another person.
- 14.14. Communicating a threat to another person or organization.
- 14.15. Displaying any prejudicial or disparaging material based on race, color, national origin, sex, religion, age, or disability.
- 14.16. Broadcasting unnecessary advertisements or personal announcements.
- 14.17. Broadcasting unsubstantiated virus warnings.
- 14.18. Any action taken while intentionally trying to be anonymous or untraceable (e.g., www.unblockict.com, uprox.com, etc.), except where an organization has specifically established an anonymous drop box in support of mission requirements.
- 14.19. Using USAFA computing and networking resources for personal or private commercial purpose or financial gain. This does not include such activities as online banking or the personal one-time sale of items by cadets.
- 14.20. Installing and using any peer-to-peer, personal proxy, or (Voice Over IP such as MagicJack, Skype (except as included in the default Microsoft Windows OS baseline), Vonage, etc.) software including, but not limited to Kazaa, Gnutella, Morpheus, MP3 Voyer, Grokster, eDonkey, CC Proxy, FreeProxy, NetConceal Anonymizer, Anonymity 4, etc.
- 14.21. Attempting to circumvent security features of the network such as firewalls and proxy servers, and using any software whose aim is to circumvent the security of the network.
- 14.22. Installing or connecting unauthorized hardware to USAFA networks or government furnished equipment. This includes all gateways, network devices (e.g., hubs, routers, wireless access points, network storage appliances, etc.), video gaming consoles, (e.g., Wii, Sony PlayStation, X-Box, etc.), personal computers that have not been authorized by 10 CS, televisions, DVRs, PDAs, Blu-Ray players, etc.
- 14.23. Configuring wireless laptops in an ad hoc or wireless peer to peer configuration, except for the purpose of sharing information in direct support of the primary Research Development Test and Evaluation of the academic and research missions of the Academy.

15. CAC Removal Lock Policy. IAW DISA Access Control In Support of Information Systems STIG, Version 2, Release 3 paragraph 3.4.4 (AC34.205: CAT II), all USAFA information systems (e.g., network device, desktop, laptop, handheld, etc.) will be configured to lock when the CAC is removed. Any exception to this policy must be submitted IAW the

USAFA IT CAB in USAFAI 33-116, paragraph 3. The 10 CS will maintain a list of approved exceptions on the 10 CS SharePoint Portal site.

16. User ID and Password Access for Administrator Accounts.

16.1. All cadet, faculty, and limited staff are authorized to receive and use the local client “administrator” account and password on their individual computers on the .EDU domain. This client-only “administrator” password must meet DoD/Air Force standards and will expire every 180 days.

16.2. Certain administrators (e.g., 10 CS CST, and some Functional System Administrators (FSA)) are authorized to use UserID and password for network access. 10 CS will approve/maintain a list of CSTs, FSAs, and System Information Assurance Officers on the 10 CS SharePoint Portal site. Only individual administrators on this list will be granted this exception and must be DoD 8570 certified.

16.3. Within USAFA/PL, the IT department is authorized to have two individuals with password enabled accounts.

16.4. Within USAFA/DF, each department is normally authorized to have two individuals with password enabled accounts (more than two individuals may be authorized during times of transition or for large departments). These accounts will be exempted from DoD 8570 training requirements and will only be used for the following purposes:

16.4.1. Join computers to the .EDU domain. This may be done after contacting the 10 CS IT Service Desk with the computer name and ensuring it is in the department’s Active Directory Organizational Unit.

16.4.2. Administering all computers within the department’s group, and only that group. i.e., When logging into a computer which is joined to the .EDU domain within the department, the account will have local administrator rights (to include the ability to change passwords) on the client computer only.

16.4.3. Mapping to the network shared drives for the installation of software found on those drives.

16.5. CSTs outside 10 CS should not normally have permissions to computers outside their own organization. If an exception is required it must be approved via the 10 CS/SCO.

16.6. Without exception, all passwords must meet password requirements defined in DISA Access Control STIG, AFMAN 33-282, paragraph 4.5.

17. IA Certification Requirements.

17.1. Any individual requiring a waiver to IA certification requirements must submit a request IAW the USAFA IT Change Management process in USAFAI 33-116, paragraph 3. All USAFA personnel with elevated network privileges are considered to be members of the IA workforce and are required to attain and maintain appropriate IA certifications IAW DoD 8570.01-M *Information Assurance Workforce Improvement Program* and AFMAN 33-285 *Information Assurance (IA) Workforce Improvement Program* with the following exceptions:

17.1.1. Cadets, faculty and limited staff are authorized to have local administrator accounts for their individual computers on the .EDU domain but are not required to

achieve Information Assurance Technician Level I certification IAW DoD 8570.01M. To mitigate any risk caused by this exception:

17.1.1.1. Cadets, faculty and limited staff are not authorized any additional elevated privileges on the .EDU network.

17.1.1.2. Cadets, faculty and staff are required to complete IA Awareness training to access USAFA network resources.

17.2. USAFA/A6 will report metrics for USAFA IA workforce compliance annually to USAFA DAA and as required IAW DoD 8570.01-M and AFMAN 33-285. This report will include identification of all IA positions, the level of certification required for IA positions, and compliance with achieving certifications.

17.3. The 10 CS will collect and track 8570 metrics and provide to USAFA/A6 monthly.

18. Guest Accounts for .EDU Network. USAFA's educational mission requirements occasionally necessitate temporary guest access to the .EDU domain.

18.1. To ensure compliance with AFI 33-115V2, *Licensing Network Users and Certifying Network Professionals*, paragraph 5.1 and AFI 33-129, paragraph 2.2.11, the following are required prior to approval of guest accounts:

18.1.1. Requests to create guest accounts must be submitted via the organization's Communications Requirements Officers (CRO) IAW the USAFA IT Change Management process in USAFAI 33-116, paragraph 3. For users/organizations without a CRO, guest account requests may be submitted directly to the USAFA IT Service Desk. The request must provide access-level requirements, justification and duration.

18.1.2. The guest must complete IA Awareness training and sign a NULA prior to being granted access to the .EDU network. Manual NULAs are authorized by 10 CS for guests.

18.2. Depending on requirements and duration, approved .EDU guests will be required to either attain a CAC or be allowed UserID/password access to the .EDU domain. If UserID/password access is approved, passwords must meet the minimum requirements in DISA Access Control STIG, AFMAN 33-282, paragraph 4.5.

18.3. The 10 CS will maintain a list of approved guest accounts and will determine the length of guest accounts (not to exceed 6 months). Only individuals on this list are granted guest accounts.

18.4. Non-US nationals (cadets, faculty and staff) are authorized access on USAFA academic and research network enclaves, provided that the appropriate visit request and security plan documentation has been approved by the IP office, as prepared by the hosting department or organization.

19. Global Address List (GAL) Title Field. IAW TO 00-33D-2001 DoD personnel titles are limited to the following: rank for military members, GS-# or Civ for DoD civilians, CTR for contractors, Ret for retired military and Mr, Ms, Miss, Mrs, Dr, HON, ESQ, etc., for civilians.

20. Internet Blocking. Due to educational and recreational requirements, approved categories may be different from those typically allowed for most DoD and AF users.

20.1. The 10 CS/SCO will maintain a list of currently approved USAFA blocked categories on the 10 CS SharePoint Portal site.

20.2. Requests for changes to the approved USAFA blocked and unblocked categories list must be submitted IAW the USAFA IT Change Management process in USAFAI 33-116, paragraph 3.

20.3. Requests for an individual site to be unblocked, should be submitted via a trouble ticket to the IT service desk.

21. Port Exceptions. The DoD Ports, Protocols, and Services Management (PPSM) program Registry Database is the only authoritative source for Ports, Protocols, and Services information. USAFA Network Administrators are responsible for the configuration of network security devices IAW the PPSM Registry Database and Category Assurance List.

21.1. The 10 CS/SCO will maintain a list of approved open ports on the shared drive and will revalidate this list annually, at a minimum.

21.2. Requests to open ports must be submitted IAW the USAFA IT Change Management process in USAFAI 33-116, paragraph 3.

22. Inactive LAN Drops (Switchports). Approved switchports in cadet living areas and academic areas will not be disabled when inactive and will allow access to multiple non-concurrent authorized devices. The following actions are required to mitigate risk associated with this exception:

22.1. Any switchport requiring this exception must be submitted IAW the USAFA IT Change Management process in USAFAI 33-116, paragraph 3.2.

22.2. The 10 CS/SCO will maintain a list of switchports approved for this exception and will revalidate this list annually, at a minimum.

22.3. The 10 CS/SCO will enable port security on any switchports not identified on the exception list.

23. BlackBerry, Personal Data Assistant (PDA) and Cell Phone Authorization.

23.1. All requests for government Blackberry smartphones, PDAs, and cell phones must be submitted and approved IAW USAFAI 33-119, paragraph 3.1 using the WOMS.

23.2. Units requesting issuance of Blackberry smartphones, PDAs, and cell phones for mission required positions, will do so using the USAFA Form 141, *Authorization for Government Blackberry, Smartphones, PDA, or Cell Phone*. As general guidance, 24x7 connectivity is often required of Commanders, Directors, Chief Master Sergeants, and First Sergeants; others shall be determined by Commanders and Directors.

23.3. The CRO will include the request template as an attachment in the WOMS. The 10 CS will order and issue mobile devices per their consolidated commercial cellular services contract.

23.4. Unit Personal Wireless Communications Systems (PWCS) Managers will maintain an inventory of these commercial mobile devices and supply the Base PWCS Manager an updated inventory annually for records reconciliation.

23.5. IAW AFI 33-106, *Managing High Frequency Radios, Personal Wireless Communication Systems, and The Military Affiliate Radio System*, paragraph 4.9.1.3., using organizations are responsible for payment of their commercial cellular bills using unit funds.

23.5.1. Effective Fiscal Year 13, decentralized billing at USAFA will be implemented by the unit government purchase card program and initial distribution of funding. Organizations must plan and program budgets for purchase, maintenance and usage of their own Blackberry smartphones, PDAs and cell phones based on forecasted need.

23.5.2. Units should not plan to pay for initial or sustainment costs using end of year funds.

23.6. IAW DoD MFR, *Use of Commercial Mobile Devices Not Connected to DoD Networks*, dated 31 July 2012, "Processing, storing, transmitting, or receiving any FOUO or non-publicly releasable data is not authorized." Mobile devices that are on the DoD Unified Capabilities Approved Products List are approved for purchase, but are not authorized for connection to any DoD-owned or DoD-funded network.

24. Television Services.

24.1. VBrick is the preferred video streaming program for all USAFA .EDU users.

24.2. IAW AFI 64-101, *Multichannel Video Programming Distribution (Broadcast Cable)*, paragraph 4.3.4.3., TV services shall be allocated and funded at the discretion of the Commanders, Directors, equivalents (or delegated office).

25. Video Teleconference (VTC).

25.1. Due to the limited number of VTCs and increased bandwidth usage, organizations are encouraged to use Defense Connect Online (DCO) whenever possible. DCO information and account registration are located at the DCO website at <https://www.dco.dod.mil>. DCO meetings conducted from the user's desktop are the preferred method for combined webinars, instant messaging, and camera based-video-voice communication.

25.2. VTC suite owners or those requesting shall:

25.2.1. Submit VTC requirements via the organization's CRO IAW the USAFA IT Change Management process in USAFAI 33-116, paragraph 3.

25.2.2. Appoint at least two VTC facilitators (primary and alternate) from within its unit and ensure that each member completes facilitator certification training IAW AFMAN 33-145, *Collaboration Services and Voice Systems Management*, paragraph 3.5. Training is accessed via the Defense Information System Network (DISN) website (<http://dvstraining.prosoft.tv/>). Training certificates will be maintained until the facilitator is reassigned.

25.2.3. Be responsible for all aspects of the equipment's lifecycle, to include funding, procurement, maintenance, housing and Enterprise Information Technology Data Repository compliance. Moreover all current and future VTC suites are subject to IA and certification and accreditation requirements IAW AF and USAFA guidelines.

25.3. Individuals from organizations without VTC facilities will request the use of a VTC suite directly from a facilitator of a VTC suite owning organization. Scheduling priority and procedures for a VTC are maintained by the unit that houses the equipment.

25.3.1. Each VTC facility will maintain a continuity book containing (at a minimum) the following documents:

- 25.3.1.1. Appointment letter of VTC facilitator (primary and alternate).
- 25.3.1.2. DISN Non-resident Phase training certificate for each facilitator.
- 25.3.1.3. VTC equipment listing.
- 25.3.1.4. Inspection requirements and results.
- 25.3.1.5. Preventative maintenance requirements (maintain records for 12 months).
- 25.3.1.6. Checklist to setting up, scheduling, and facilitating a VTC.
- 25.3.1.7. Applicable Information Assurance documentation (Authority to Operate letter and Emissions Security approval, etc.).

26. Internet Service Requirements. In order to facilitate mission accomplishments and protect government resources from malicious sites, all organizations requiring Internet Services (purchased with Government funds) beyond the USAFA Enclave must submit a WOMS ticket via the organization's CRO IAW the USAFA IT Change Management process in USAFAI 33-116, paragraph 3.

26.1. Only cadet-owned computing devices, government procured computing devices and members of the press/media owned devices will be allowed to connect to the Internet Services (e.g., Comcast, Verizon, etc.). The computing devices must be sanitized prior to initial use to remove all official use only and/or sensitive but unclassified information before connecting.

26.1.1. Internet Service computing devices must maintain physical and logical separation from the government network infrastructure.

26.1.2. Users will protect Internet Service computing devices with available firewalls and antivirus software (e.g., McAfee or Norton Antivirus). Exceptions are allowed for some academic mission requirements (i.e. Cyber Training Range).

26.2. Upon receipt of approval, all organizations must sign a USAFA Form 142, *USAFA Commercial ISP Agreement*, draft a waiver request letter (Attachment 3) and submit a request to their Commander or Director (or equivalent) for validation.

26.3. Requesting organizations that are approved to procure Internet Services are responsible for budgeting and funding all initial and recurring charges necessary to maintain Internet services, including stand-alone computers to access the internet via a commercial provider. The 10 CS will not install/maintain user internet service equipment/infrastructure.

MICHAEL C. GOULD, Lt Gen, USAF
Superintendent

Attachment 1**GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION*****References***

Federal Information Security Management Act (FISMA)

CJCSI 6211.02, *Defense Information Systems Network (DISN): Policy and Responsibilities*

DoD 5400.7-R_AFMAN 33-202, *Freedom of Information Act Program*

DoD 5500.7-R, *Joint Ethics Regulation (JER)*

DoD 8570.01-M, *Information Assurance Workforce Improvement Program*

DoDI 8100.04, *DoD Unified Capabilities (UC)*

DoDI 8500.2, *Information Assurance (IA) Implementation*

Defense Federal Acquisition Regulation (DFAR) Supplement, Part 208, *Required Sources of Supplies and Service*, Subpart 208.74, *Enterprise Software Agreements (ESA)*

SECDEF Directive-Type Memorandum (DTM) 09-026, *Responsible and Effective Use of Internet-based Capabilities*, (<http://www.dtic.mil/whs/directives/corres/pdf/DTM-09-026.pdf>)

AFI 33-101, *Commanders Guidance and Responsibilities*

AFI 33-102, *Communications and Information Specialized Publications*

AFI 33-106, *Managing High Frequency Radios, Personal Wireless Communication Systems, and the Military Affiliate Radio System*

AFI 33-112, *Information Technology Hardware Asset Management*

AFI 33-115 Volume 2, *Licensing Network Users and Certifying Network Professionals*

AFI 33-129, *Web Management and Internet Use*

AFI 33-210, *Air Force Certification & Accreditation (C&A) Program (AFCAP)*

AFI 33-321, *Authentication of Air Force Records*

AFI 33-322, *Records Management Program*

AFI 33-332, *Air Force Privacy Program*

AFI 33-360, *Publications and Forms Management*

AFI 33-364, *Records Disposition – Procedures and Responsibilities*

AFI 35-101, *Public Affairs Responsibilities and Management*

AFI 35-107_USAFASUP, *Public Web Communications*

AFH 33-337, *Tongue and Quill*

AFMAN 33-145, *Collaboration Services and Voice Systems Management*

AFMAN 33-152, *User Responsibilities and Guidance for Information Systems*

AFMAN 33-282, *Computer Security (COMPUSEC)*

AFMAN 33-285, *Information Assurance (IA) Workforce Improvement Program*

AFMAN 33-363, *Management of Records*

AFPD 33-1, *Cyberspace Support*

USAFAI 33-115, *Information Technology Service Configuration Management*

USAFAI 33-116, *Information Technology Change Management*

USAFAI 33-119, *Information Technology Service Operations Management*

690th Network Support Group (690 NSG) Special Instruction – 1 (SPIN-1)

DISA Security Technical Implementation Guides (STIG)

Technical Order (TO) 00-33D-2001

Prescribed Forms

USAFA Form 136, *Software Request Questionnaire*

USAFA Form 141, *Authorization for Government Blackberry, Smartphone, PDA, or Cell Phone*

USAFA Form 142, *USAFA Commercial ISP Agreement*

Adopted Forms

AF Form 847, *Recommendation for Change of Publication*

AF Form 4394, *Air Force User Agreement Statement – Notice and Consent Provision*

DD Form 2875, *System Authorization Access Request*

Abbreviations and Acronyms

AF—Air Force

AFMAN—Air Force Manual

AFPD—Air Force Policy Directive

AFRIMS—Air Force Records Information Management System

CAB—Change Advisory Board

CAC—Common Access Card

COTS—Commercial-Off-The-Shelf

CRO—Communication Requirement Officers

CS—Communications Squadron

CST—Client Systems Technicians

DAA—Designated Accrediting Authority

DCO—Defense Connect Online

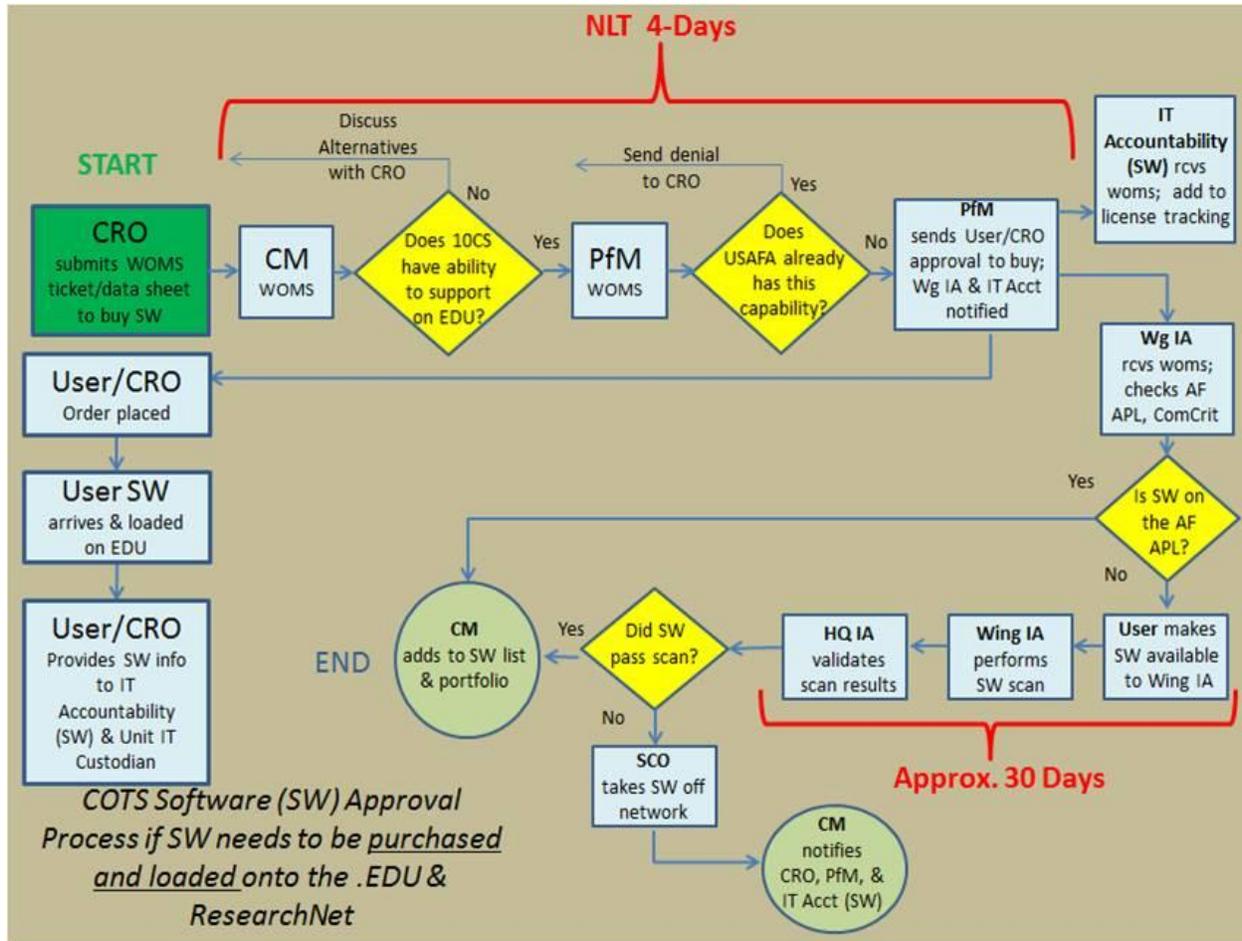
DISA—Defense Information Systems Agency

DISN—Defense Information System Network

DOD—Department of Defense
DPI—Digital Printing and Imaging
DRU—Direct Reporting Unit
FSA—Functional System Administrator
GAL—Global Address List
IA—Information Assurance
IAW—In Accordance With
IT—Information Technology
ITFWG—IT Financial Working Group
LCR—Life Cycle Replacement
MP—Mission Partner
NULA—Network Users License Agreement
PA—Public Affairs
PDA—Personal Data Assistant
PII—Personally Identifiable Information
PKI—Public Key Infrastructure
PPSM—Ports, Protocols, and Services Management
PWCS—Personal Wireless Communications Systems
SSL—Secure Socket Layer
STIG—Security Technical Implementation Guide
USAFA—United States Air Force Academy
VPN—Virtual Private Network
VTC—Video Tele-Conferencing
WOMS—Work Order Management System

Attachment 2

COTS SOFTWARE APPROVAL PROCESS



Attachment 3**REQUIREMENTS FOR COMMERCIAL ISP LETTER**

YOUR LETTER HEAD

DATE

MEMORANDUM FOR 10 CS

FROM: (INSERT YOUR ORGANIZATION)

SUBJECT: Request Approval for Procurement and Use of Commercial Internet Services

1. Request approval for government funded commercial internet service for official use. Our organization is required to connect to the commercial internet service in support of XXXXXX. We are unable to connect via the .EDU or .MIL network due to XXXXX.
2. Cost data is ~ \$XXXX first year + start-up; and ~ \$XXX annually thereafter.
3. I acknowledge that we have budgeted for the CISP resources.

YOUR COMMANDERS SIGNATURE
BLOCK