DEPARTMENT OF THE AIR FORCE
WASHINGTON D.C.

Office Of The Secretary

AFI 33-100_AFGM 1

MAY 3 2010

MEMORANDUM FOR DISTRIBUTION C
MAJCOMs/FOAs/DRUs

FROM: SAF/CIO A6
1800 Air Force Pentagon
Washington DC 20330-1800

SUBJECT: Air Force Guidance Memorandum to AFI 33-100, *User Responsibilities and Guidance for Information Systems*

References: (a) Directive-Type Memorandum (DTM) 09-026, *Responsible and Effective Use of Internet-based Capabilities*, February 25, 2010.
http://www.dtic.mil/whs/directives/corres/pdf/DTM-09-026.pdf
(b) DOD 5500.7-R, *Joint Ethics Regulation*, August 1, 1993
(c) through (j), see Attachment 1

This is an Air Force Guidance Memorandum immediately changing AFI 33-100, *User Responsibilities and Guidance for Information Systems*. Compliance with this Memorandum is mandatory. To the extent its directions are inconsistent with other Air Force publications, the information herein prevails, in accordance with AFI 33-360, *Publications and Forms Management*.

Failure to observe the prohibitions and mandatory provisions of this instruction as stated in Attachment 2, paragraph 2.1 by military personnel is a violation of the *Uniform Code of Military Justice* (UCMJ), Article 92, Failure to Obey Order or Regulation. Violations by ANG military personnel may subject members to prosecution under their respective State Military Code or result in administrative disciplinary action without regard to otherwise applicable criminal or civil sanctions for violations of related laws. Violations by civilian employees may result in administrative disciplinary action without regard to otherwise applicable criminal or civil sanctions for violations of related laws. Violations by contactor personnel will be handled according to local laws and the terms of the contract.

Compliance with DTM 09-026 for the responsible and effective use of Internet-based capabilities is mandatory. Internet-based capabilities are defined as all publicly accessible information capabilities and applications available across the Internet in locations not owned, operated, or controlled by the Air Force, Department of Defense, or the Federal Government. Internet-based capabilities include collaborative tools such as social networking services (SNS), social media, user-generated content, social software, e-mail, instant messaging, and discussion forums (e.g., YouTube, Facebook, MySpace, Twitter, Google Apps).

In accordance with DTM 09-026, Air Force personnel are authorized official use and limited personal use of Internet-based capabilities via Air Force-owned and/or -operated IT. This usage includes Internet resources and services (including data and systems) that provide information or two-way communication (dialogue) with the public. All users must follow the specific guidelines defined in DTM 09-026 and in Attachment 2.

External official presences using Internet-based capabilities are allowed. An external official presence is defined as official public affairs activities conducted on non-DoD sites on the Internet (e.g., Combatant Commands on Facebook, Chairman of the Joint Chiefs of Staff on Twitter). SAF/PA will release separate public affairs guidance and/or policy.

All Internet-based capabilities whose purpose clearly involves prohibited content shall continue to be blocked. Prohibited is content that is inappropriate, including: adult content, sexually explicit or sexually oriented material, nudity, hate speech or ridicule of others on the basis of protected class (e.g., race, creed, religion, color, age, sex, disability, national origin), gambling, illegal weapons, militancy/extremist activities, terrorist activities, and any other content or activities that are illegal or inappropriate.

Classified, For Official Use Only, Controlled Unclassified Information, Critical Information, and/or personally identifiable information will not be posted on DoD-owned, -operated, or -controlled publicly accessible sites or on commercial Internet-based capabilities. All users must strictly adhere to sound operations security (OPSEC) practices, as stipulated in AFI 10-701, *Operations Security*, and users are responsible for following information assurance and OPSEC guidance provided in all education, training, and awareness activities.

The guidance in this Memorandum becomes void after 180 days have elapsed from the date of this Memorandum, or upon incorporation by interim change to, or a rewrite of AFI 33-100, whichever is earlier.

W. T. Lord

WILLIAM T. LORD, Lt Gen, USAF
Chief of Warfighting Integration and
Chief Information Officer

2 Attachments:
1. References
2. Responsible and Effective Use of Internet-based Capabilities

Attachment 1

REFERENCES

(c) AFI 33-100, *User Responsibilities and Guidance for Information Systems*, 19 Nov 2008
(d) AFI 33-129, *Web Management and Internet Use*, 25 Feb 2005
(e) AFI 10-701, *Operations Security*, 18 Oct 2007
(f) AFI 33-322, *Records Management Program*, 7 Oct 2003
(g) AFI 33-364, *Records Disposition-Procedures and Responsibilities*, 22 Dec 2006
(h) AFI 33-332, *Privacy Act Program*, 29 Jan 2004
(i) AFMAN 33-363, *Management of Records*, 1 Mar 2008
(j) AFI 33-360, *Publications and Forms Management*, 18 May 2006

Attachment 2

RESPONSIBLE AND EFFECTIVE USE OF INTERNET-BASED CAPABILITIES

1. **Limited Authorized Personal Use.** AFI 33-100, paragraph 6.2.2. is hereby replaced with the following:

1.1. Government-provided hardware and software are for official use and limited authorized personal use only. Limited personal use must be of reasonable duration and frequency that have been approved by supervisors and do not adversely affect performance of official duties, overburden systems or reflect adversely on the AF or the DoD.

1.1.1. All personal use must be consistent with the requirements of DOD 5500.7-R, *Joint Ethics Regulation.*

1.1.2. When accessing Internet-based capabilities using Federal Government resources in an authorized personal or unofficial capacity, individuals shall comply with OPSEC guidance (AFI 10-701) and shall not represent the policies or official position of the AF or the DoD.

1.1.3. Examples of authorized limited personal use include, but are not limited to:

1.1.3.1. Notifying family members of official transportation or schedule changes.

1.1.3.2. Using government systems to exchange important and time-sensitive information with a spouse or other family members (i.e., scheduling doctor, automobile, or home repair appointments, brief Internet searches, or sending directions to visiting relatives).

1.1.3.3. Educating or enhancing the professional skills of employees, (i.e., use of communication systems, work-related application training, etc.).

1.1.3.4. Sending messages on behalf of a chartered organization, (i.e., organizational Booster Club, Base Top 3, Base Company Grade Officers Association, etc.).

1.1.3.5. Limited use by deployed members for morale, health, and welfare purposes.

1.1.3.6. Job searching.

2. **Inappropriate Use.** AFI 33-100, paragraph 3.9.1. is hereby replaced with the following:

2.1. Using the Internet for other than official or limited authorized personal purposes may result in adverse administrative or disciplinary action. The activities listed in paragraphs 2.1.1. through 2.1.13. involving the use of government-provided computer hardware or software are specifically prohibited. **Failure to observe the prohibitions and mandatory provisions of these paragraph by military personnel is a violation of the *Uniform Code of Military Justice (UCMJ)*, Article 92, Failure to Obey Order or Regulation. Violations by ANG military personnel may subject members to prosecution under their respective**

State Military Code or result in administrative disciplinary action without regard to otherwise applicable criminal or civil sanctions for violations of related laws. Violations by civilian employees may result in administrative disciplinary action without regard to otherwise applicable criminal or civil sanctions for violations of related laws. Violations by contactor personnel will be handled according to local laws and the terms of the contract.

2.1.1. Use of Federal government communications systems for unauthorized personal use.

2.1.2. Uses that would adversely reflect on the DoD or the AF such as chain letters, unofficial soliciting, or selling except on authorized Internet-based capabilities established for such use.

2.1.3. Unauthorized storing, processing, displaying, sending, or otherwise transmitting prohibited content. Prohibited content includes: adult content, sexually explicit or sexually oriented material, nudity, hate speech or ridicule of others on the basis of protected class (e.g., race, creed, religion, color, age, sex, disability, national origin), gambling, illegal weapons, militancy/extremist activities, terrorist activities, and any other content or activities that are illegal or inappropriate.

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

2.1.5. Using copyrighted material in violation of the rights of the owner of the copyrights. Consult with the servicing Staff Judge Advocate for "fair use" advice.

2.1.6. Unauthorized use of the account or identity of another person or organization.

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

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

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

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

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

2.1.12. Copying and posting of For Official Use Only, Controlled Unclassified Information, Critical Information, and/or personally identifiable information on DoD-

owned, -operated, or -controlled publicly accessible sites or on commercial Internet-based capabilities.

2.1.13. Downloading and installing freeware/shareware or any other software product without Designated Approving Authority (DAA) approval.

3. **Official Use.** AFI 33-100, paragraph 6.2.1.1.8. is hereby rescinded.

3.1. Pertaining to AFI 33-100, paragraph 6.2.1., official uses of Internet-based capabilities unrelated to public affairs are permitted. However, because these interactions take place in a public venue, personnel acting in their official capacity shall maintain liaison with their public affairs and operations security staff to ensure organizational awareness. Use of Internet-based capabilities for official purposes shall:

3.1.1. Comply with references (e) through (i).

3.1.2. Be consistent with the requirements of DOD 5500.7-R.

3.1.3. Comply with public affairs Internet-based capabilities guidance.

3.1.4. Ensure that the information posted is relevant and accurate and provides no information not approved for public release, including personally identifiable information (PII).

3.1.5. Provide links to official AF content hosted AF-owned, -operated, or -controlled sites where applicable.

3.1.6. Include a disclaimer when personal opinions are expressed (e.g., "This statement is my own and does not constitute an endorsement by or opinion of the Air Force or the Department of Defense").

4. **Records management.** Records management will be established as applicable for Air Force External Official Presence and for AF-owned, -operated, or -controlled publicly accessible Internet sites. All use must comply with references (f) through (i).

BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 33-100

19 NOVEMBER 2008

Incorporating Change 1, 23 June 2009

Communications and Information

USER RESPONSIBILITIES AND GUIDANCE FOR INFORMATION SYSTEMS

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: SAF/XCPP

Certified by: SAF/XCP-2
(Col Robert Skinner)
Pages: 36

This instruction implements Air Force Policy Directive (AFPD) 33-1, *Information Resources Management*, AFPD 33-2, *Information Assurance (IA) Program*, and identifies policies and procedures for the use of communications and information (C&I) systems/services and compliance requirements of Secretary of the Air Force, Chief of Warfighting Integration and Chief Information Officer (SAF/XC) managed programs. These programs ensure availability, interoperability, and maintainability of C&I systems/services in support of Air Force mission readiness and warfighting capabilities. This publication applies to all military and civilian Air Force personnel, members of the Air Force Reserve and Air National Guard, and other individuals or organizations as required by binding agreement or obligation with the Department of the Air Force. **Failure to observe the prohibitions and mandatory provisions of this instruction as stated in paragraph 3.9.1., 4.5.4.2.1., 4.11.1., 6.2.1.1.1. through 6.2.1.1.8, 6.2.3.1., and 7.1.1.2. by military personnel is a violation of the *Uniform Code of Military Justice (UCMJ)*, Article 92, Failure to Obey Order or Regulation. Violations by civilian employees may result in administrative disciplinary action without regard to otherwise applicable criminal or civil sanctions for violations of related laws. Violations by contactor personnel will be handled according to local laws and the terms of the contract. Additionally violations of paragraph 3.9.1. by ANG military personnel may subject members to prosecution under their respective State Military Code or result in administrative disciplinary action without regard to otherwise applicable criminal or civil sanctions for violations of related laws.** Direct questions or comments on the contents of this instruction, through appropriate command channels, to Air Force Communications Agency (HQ AFCA/EASD), 203 W. Losey Street, Room 1100, Scott AFB IL 62225-5222. Send recommended changes and conflicts between this and other publications, using Air Force (AF)

Form 847, *Recommendation for Change of Publication*, to HQ AFCA/EASD, with an information copy to the Office of the Secretary of the Air Force for Warfighting Integration and Chief Information Officer, Policy and Governance Division (SAF/XCPP), 1800 Air Force Pentagon, Washington DC 20330-1800. Ensure that 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 Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS) located at **https://afrims.amc.af.mil/rds_series.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.

SAF/XC is changing all their publications from "stove-piped" system/program based to audience/role based by consolidating like information from existing Air Force instructions (AFIs). The initial targets for consolidations are based around general users, commanders, implementers, and support enablers. During this phase, the consolidation will address the first three audiences. Existing AFIs will retain support enabler information containing detailed system/program guidance and/or procedural information. The information contained in this publication was extracted from the publications identified in **Attachment 5**.

SUMMARY OF CHANGES

This interim change implements DoD CIO Memorandum, 9 May 2008, *Policy on Use of Department of Defense (DoD) Information Systems-Standard Consent Banner and User Agreement.* All Users of DoD information systems will sign the standardized AF Form 4394, *Air Force User Agreement Statement-Notice and Consent Provision.* It also corrects out dated references to AFI 33-202v1, that was superseded by AFI 33-200.

1. Introduction.

1.1. In an effort to meet the growing needs of today's warfighter, great strides are being made to improve the capabilities offered by the Air Force provisioned portion of the Global Information Grid (GIG). Today's Air Force is increasingly using these capabilities in almost all activities of warfighting and operations support. This increased reliance on technology and its integration requires each individual to take responsibility for ensuring effective, efficient, and authorized use of these resources as they carry out their responsibilities.

2. Network and Information System Access.

2.1. **Access Control.** Access control is one of the measures taken to ensure Information Systems (ISs) are protected against threats and vulnerabilities. To control ISs access, identification and authentication techniques and procedures are used. The two IS access control methods used are the Common Access Card (CAC) with a Personal Identification Number (PIN) or a username with password.

2.1.1. CAC. The CAC is the DoD identification card and is used to digitally sign electronic messages, travel orders, travel vouchers, and other documents and establish secure web-based sessions. See AFI 36-3026(I), *Identification Cards for Members of the Uniformed Services, Their Eligible Family Members, and Other Eligible Personnel,* for additional information.

2.1.1.1. Users must not share their PIN and must protect their CAC from unauthorized access at all times. A user who suspects that these have been compromised must notify their organizational Information Assurance Officer (IAO) or Client Support Administrator (CSA) immediately.

2.1.2. Username with Password. Some ISs are not CAC-enabled and use a username and password for access.

2.1.2.1. Password Composition. All passwords must be a minimum of nine characters. Passwords must contain a mix of at least two lowercase letters, two uppercase letters, two numbers, and two special characters. Passwords must not contain dictionary words spelled frontward or backward, slang words, names of persons, places or things, including derivatives or modifications of such words, or split with a number or special character. The passwords must not be patterns of letters

on the keyboard, must not contain any personal identity (to include username or user-id), history, or environment, and must not mimic previous passwords. (See **Attachment 4** for additional information).

2.1.2.2. Password Protection. Each user is responsible and accountable for their password.

2.1.2.2.1. Memorize your password. Do not place passwords on desks, walls, sides of terminals, or store them in a function key, log-in script, batch file, or other communications software. If documentation is necessary for mission accomplishment (i.e., pre-established accounts for contingency or exercise), place the password in a properly marked, sealed envelope and store it in a safe. In the case of web-based log-in, the fact that an individual user has authenticated can be tracked for that session only (i.e., through the use of nonpersistent cookies or preferences) but the actual password used cannot be stored or passed on.

2.1.2.2.2. Upon initial access to an information system, each user must enter his username and password. A user must enter a password in such a manner that the password is not revealed to anyone observing the entry process.

2.1.2.2.3. Do not share your password. If password sharing is necessary for mission accomplishment, ensure the password is changed immediately after shared access is no longer required.

2.1.2.3. Password Classification. Protect all passwords based on the sensitivity of the information or critical operations they protect (i.e., a password used to gain access to a SECRET network is itself classified SECRET). At a minimum, you must safeguard all passwords as "For Official Use Only" (FOUO).

2.2. **Training Requirement.** All Air Force military, civilian, and contractors will receive documented Information Assurance (IA) training prior to receiving access to the IS. Contact your CSA for the required training.

2.3. **Favorable Background Investigation.** All individuals accessing the Air Force Global Information Grid (AF-GIG) must meet the investigative requirements of AFI 31-501, *Personnel Security Management Program*.

2.4. **Loss of Security Clearance.** If an individual's security clearance is suspended or revoked, access to IS may be suspended. If an organizational commander feels the member should have access restored on an interim basis, they shall follow waiver request procedures outlined in AFI 33-200, *Information Assurance (IA) Management*).

2.5. Access Suspension. User's conduct inconsistent with the Air Force Information Assurance (IA) principles, may experience suspension of access to IS.

2.5.1. Actions inconsistent with IA principles include, but are not limited to:

2.5.1.1. Failure to maintain an acceptable level of proficiency on a critical program (based upon determination by the system's Designated Accrediting Authority [DAA] or Information System Owner [ISO])

2.5.1.2. Actions that threaten the security of a network or a governmental communications system

2.5.1.3. Actions that may result in damage or harm to a network or governmental communications system

2.5.1.4. Actions that constitute unauthorized use under the provisions in **paragraph 3.9.1.** in this instruction.

2.5.2. Once the violation is confirmed, the user is notified in writing of the access suspension by their commander (or designee), including the specific reason for the suspension and the steps the user must take to have access reinstated. The user may accept the suspension or dispute the grounds for the suspension by providing a written request for reconsideration within three duty days. Dispute resolution and interim access to information systems will be processed according to AFI 33-200.

2.5.3. The user will reaccomplish appropriate training prior to reinstatement of access to IS.

3. Information Technology (IT) and Information Systems.

3.1. General Guidelines.

3.1.1. Appropriate Use. All government communications systems are subject to monitoring, interception, search, and seizure for all authorized purposes, reference DoD Chief Information Officer (CIO) Memorandum, *Policy on Use of Department of Defense (DoD) Information Systems Standard Consent Banner and User Agreement*, dated 9 May 2008. Government-provided hardware and software are for official use and authorized purposes only. Appropriate officials may authorize personal uses consistent with the requirements of DoD 5500.7-R, *Joint Ethics Regulation (JER)*, after consulting with their ethics counselor. Such policies should be explicit, as unofficial uses that exceed the authorized purposes may result in adverse administrative or disciplinary action. For guidance on the use of the Internet, see **paragraph 3.9.** Using Internet and IT Resources.

3.1.2. Report unauthorized network activities or incidents to the CSA or ISO to ensure notification continues up the chain of command.

3.1.3. Do not input or store government information on privately owned IS and media without specific approval of the DAA. Contact your CSA or ISO for assistance.

3.1.4. Do not operate any wireless technology, devices or service (used for storing, processing, and/or transmitting information), in areas where classified information is discussed, electronically stored, electronically processed, or electronically transmitted without approval of the installation Emission Security (EMSEC) manager.

3.1.5. Lost or stolen government wireless devices must be reported immediately to your CSA or ISO.

3.2. Acquiring Information Technology (IT) Assets.

3.2.1. Adhere to locally defined requirements process when acquiring IT assets. The installation Communications and Information Systems Officer (CSO) supports the information systems requirements process enabling requesting organizations to obtain new communications and information capabilities.

3.2.2. Acquire desktop computers and laptops IAW established acquisition policy.

3.3. **Communications and Information System Relocations or Modifications.**

3.3.1. The CSO must be involved in all projects involving communications and information infrastructure or assets.

3.3.2. The user submits requests in accordance with organization policy before initiating any project to install, relocate, modify, or remove communication and information systems.

3.4. **Portable Electronic Devices (PED).** PED is a generic title used to describe the myriad of small electronic items (e.g. Personal Digital Assistants (PDAs), Cellular Telephones (CTs), two-way pagers, audio/video recording devices, and hand-held/laptop computers) widely available. Almost all have wireless telecommunications capabilities that offer tremendous advantages for government users. It is becoming difficult to differentiate between these electronic devices, as the trend is to combine capabilities and functions in various forms and format. PED users must:

3.4.1. Comply with Air Force IS operating instructions. Contact your ISO or CSA for assistance.

3.4.2. Connecting non-government-owned PEDs to an Air Force network is prohibited. If individuals have a requirement to use a PED on an Air Force network, they must request issuance of a government-owned PED.

3.4.3. Encrypt data transmitted through a commercial or wireless network (data-in-transit).

3.4.4. Protect data stored or processed by the PED against tampering, theft, and loss.

3.4.5. Encrypt all stored information (data-at-rest) not otherwise approved for public release. Contact your CSA for approved procedures for encrypting. Contact your Freedom of Information Act Officer or Public Affairs Officer for information on determining what information is releasable to the public.

3.4.6. Obtain DAA approval before using a PED for storing or processing High Impact Personally Identifiable Information (PII) (see Terms, **Attachment 1**). Restrict use to protected workplaces (see Terms, **Attachment 1**). PEDs taken outside protected workplaces must adhere to the following additional security requirements:

3.4.6.1. The PED must be signed in and out of protected workplaces with a supervising official (for logging and tracking procedures).

3.4.7. Not use wireless-enabled PEDs for storing, processing or transmitting classified information without explicit written approval of the DAA and cognizant security authority.

3.4.7.1. If the PED is for classified use, encrypt transmission (data-in-transit) of the information using approved cryptography. Follow information security requirements for physically controlling and safeguarding the device and information according to AFI 31-401, *Information Security Program Management*.

3.4.7.2. In the event classified information is processed or maintained on an unclassified PED, the individual discovering the incident will immediately notify their CSA or ISO.

3.4.8. Do not connect PEDs to more than one network at a time. PEDs connected directly to a Department of Defense (DoD)-wired network (e.g., via a hot synch connection to a workstation) must not be permitted to operate wirelessly.

3.4.9. Do not use wireless-enabled PEDs in areas where classified information is discussed or processed without coordination from the installation EMSEC manager.

3.4.10. Do not enable wireless capability unless necessary for the mission and approved by the DAA.

3.4.11. Immediately report lost or stolen PEDs to the CSA or ISO.

3.5. **Removable Information Systems Storage Media Control.** Removable media refers to information system storage media that can be removed from its reader device, conferring portability on the data it carries (e.g., diskettes, CDs, Universal Serial Bus (USB) storage devices, or any other device on which data is stored and which normally is removable from the system by the user or operator).

3.5.1. Safeguard, mark, and label removable media according to the requirements for the highest level of information ever contained on the media using applicable information security guidance in AFI 31-401 and AFI 33-332, *Privacy Act Program*. Additionally follow external and internal labeling guidance in AFMAN 33-363.

3.5.2. Restrict the use of removable media containing controlled unclassified information (CUI) (see Terms, **Attachment 1**).

3.5.2.1. Removable media shall not be removed from protected workplaces unless encrypted and signed in and out with a supervising official. (See **paragraph 7.1.1.5.** for additional details on encryption.)

3.5.3. Removable media containing High Impact PII (see Terms, **Attachment 1**) requires DAA approval.

3.5.4. Immediately report loss or suspected loss of removable media containing CUI or PII to CSA or ISO.

3.5.5. Clear, sanitize, or destroy removable media used to store sensitive information before release to unauthorized personnel or outside DoD control. Contact the organizational Information Assurance Officer (IAO) for assistance.

3.5.6. Obtain approval from the organizational IAO before attaching a Universal Serial Bus (USB) storage device to an IS. These devices include but are not limited to memory sticks, jump drives, and Zip drives.

3.5.6.1. Using disguised USB storage devices (designed to look like anything other than a USB storage device, e.g., watch, pen, flashlight) is prohibited.

3.5.7. Users are responsible for backing up their data stored locally on their IT system (e.g. desktop computer). Local policy may indicate the frequency or limitations of backing up data.

3.5.8. Unclassified media introduced into a classified computer becomes classified at the same classification level as the system. Limited exceptions may exist as approved by the system DAA in the systems accreditation package according to AFI 33-200.

3.6. **Wireless Devices.** Wireless devices (i.e. mice, keyboards, etc.) are widely available and use various wireless technologies to transmit data to the computer. Consult with your CSA for proper configuration. When used in areas where classified information is processed, they must be approved by the installation EMSEC manager.

3.7. **Privately Owned information system** (i.e., hardware or software) in Government and non-Government facilities. Storage of controlled unclassified information on personally owned information systems is prohibited.

3.7.1. Classified Processing. Do not use privately-owned information systems to process classified information. Privately-owned information systems contaminated with classified information will be confiscated and sanitized.

3.7.2. Unclassified and Sensitive Processing. 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 DAA approval. Justification must include mission requirement, government availability, and rationale as to why privately-owned information systems must be used.

3.8. **Public computing facilities.** Do not use public computing facilities (Internet cafés and kiosks, hotel business centers, etc.) for processing government-owned unclassified, sensitive or classified information. Public computing facilities include any information technology resources not under your private or the United States (US) Government's control. Using these resources to access web-based government services (e.g. MyPay) constitutes a compromise of log-in credentials and must be reported to your CSA.

3.9. **Using Internet and Information Technology (IT) Resources.**

3.9.1. Inappropriate Use. Using the Internet for other than official or authorized use may result in adverse administrative or disciplinary action. The activities listed in **paragraphs 3.9.1.1.** through **3.9.1.14.** involving using government-provided computer hardware or software is specifically prohibited. **Failure to observe the prohibitions and mandatory provisions of these paragraphs by military personnel is a violation of the *Uniform Code of Military Justice (UCMJ),* Article 92, Failure to Obey Order or Regulation. Violations by civilian employees may result in administrative disciplinary action without regard to otherwise applicable criminal or civil sanctions for violations of related laws**. **Violations by contactor personnel will be handled according to local laws and the terms of the contract. Violations by ANG military personnel may subject members to prosecution under their respective State Military Code or result in administrative disciplinary action without regard to otherwise applicable criminal or civil sanctions for violations of related laws.**

3.9.1.1. Using Federal government communications systems for unauthorized personal use.

3.9.1.2. Uses that would adversely reflect on the DoD or the Air Force such as chain letters, unofficial soliciting, or selling, except on authorized bulletin boards established for such use.

3.9.1.3. Unauthorized 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; sexually harassing materials, pornography and other sexually explicit materials.

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

3.9.1.5. Knowingly using copyrighted material in violation of the rights of the owner of the copyrights. Consult with the servicing Staff Judge Advocate for "fair use" advice.

3.9.1.6. Participating in non-DoD or nongovernment "chat lines," "chat groups," "blogs," or open forum discussion to or through a public site, unless it is for official purposes and approved through SAF/XCP and DoD Global Information Grid (GIG) Waiver Board.

3.9.1.7. Unauthorized use of the account or identity of another person or organization.

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

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

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

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

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

3.9.1.13. Copying and posting official information to unauthorized Web sites.

3.9.1.14. Downloading and installing freeware/shareware or any other software product without DAA approval.

3.10. **Air Force User Agreement Statement – Notice and Consent Provision.**

3.10.1. In accordance with the DoD Chief Information Officer (CIO) Memorandum, *Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement*, 9 May 2008, all users of DoD information systems will sign the standardized AF Form 4394. Commanders should restrict access to DoD information systems for those personnel who fail to sign the agreement.

3.10.2. CSAs or IAOs will keep the user agreement on file, and will ensure a copy is on file before allowing access for new members.

4. Voice Communications Services.

4.1. **Calls From Base Telephones.**

4.1.1. Use the following Defense Switched Network (DSN) and Commercial network access digits: 94 DSN ROUTINE; 98 COMMERCIAL LONG DISTANCE; 99 COMMERCIAL LOCAL.

4.1.2. Do not discuss classified information over an unsecured telephone.

4.1.3. Long Distance Calls From Base Telephones.

4.1.3.1. Use the Defense Switched Network (DSN), not commercial long distance carriers, to call other DoD activities unless DSN service is not available in a timely manner. Use the DSN system only for official business or when in the best interest of the government.

4.1.3.2. User will contact their Telephone Control Officer (TCO) to obtain a personal identification number (PIN) for accessing commercial long distance voice service. This service is authorized for official uses only.

4.1.3.3. Callers without direct long distance dialing capability must request a control or billing account number from their TCO. Give the control or billing account number to the base switchboard operator when making a call.

4.1.3.4. For verification purposes, document all commercial long distance calls on AF Form 1072, *Authorized Long Distance Telephone Calls*. This is only required when PINs are not established or the host base does not have the capability to capture source Caller ID information for each call.

4.2. **Collect Calls to Base Telephones.**

4.2.1. The installation commander provides local guidance for official collect calls.

4.3. **Personal Calls Over Official Telephones.**

4.3.1. All government communications systems are subject to monitoring, interception, search, and seizure for all authorized purposes, reference DoD Chief Information Officer (CIO) Memorandum, *Policy on Use of Department of Defense (DoD) Information Systems Standard Consent Banner and User Agreement*, dated 9 May 2008. Commanders and supervisors may allow personal calls during work hours using official telephones if:

4.3.1.1. The telephone call does not interfere with official duties.

4.3.1.2. The calls do not exceed reasonable duration and frequency, and whenever possible, are made during the employee's personal time such as after-duty hours or lunch periods.

4.3.1.3. The telephone calls serve a legitimate public interest (such as usage reduces time away from the work area or improves unit morale).

4.3.1.4. The telephone call does not reflect adversely on DoD or the Air Force (e.g., uses involving pornography; unofficial advertising, soliciting, or selling; and discussion of classified information).

4.3.1.5. The government does not incur any long distance or per-call charges above and beyond normal local charges. Normal local charges are based upon historical averages.

4.3.1.6. Personal calls may be made for "morale purposes" during Deployments and TDYs as authorized by the organizational commander, see **paragraph 4.9.** for specific guidance.

4.4. **Cordless Telephones Guidance.**

4.4.1. The installation CSO, or designated representative, approves the use of cordless telephones on a case-by-case basis. For security purposes, the use of cordless phones on military installation work centers are highly discouraged. Conversations from cordless telephones can easily be intercepted as well as "stepped-on" due to limited frequency allocation and overlapping of voice frequencies. Cordless telephones used outside the United States and Possessions (US&P) will be host nation approved.

4.4.2. Limit cordless phone use to non-command and control (C2) users and in buildings where operating cordless telephones are fully warranted by the mission and do not pose an Operations Security (OPSEC) risk.

4.4.3. Operating cordless phones within a classified environment will be approved by the installation emission security (EMSEC) manager.

4.5. **Commercial Cellular Telephone (CT) Service.**

4.5.1. Organizations must request host base CSO approval before purchasing commercial cellular equipment.

4.5.2. Personal calls to CT service providers from the host base official service may be authorized if the Air Force does not incur a long-distance toll or per-call charge. Cellular telephone services that provide per-call charges by billing the originating (calling) party, should be limited by the host base voice information system to official calls only.

4.5.3. Official Use of CT Service.

4.5.3.1. Use CT services only when it is the most cost-effective way to provide necessary communications or mobility is required.

4.5.3.2. Do not use an unclassified CT for C2 purposes. For security purposes, use a regular telephone (land line) as a first priority when and where available.

4.5.3.3. Do not transmit classified information over unsecured CTs.

4.5.3.4. Use government-issued CTs while driving on or off base according to local policies.

4.5.4. Personal Use of CT Service.

4.5.4.1. The same rules that govern use of land line telephones apply to the use of Air Force CTs. Reference **paragraph 4.9.** for official and authorized purposes.

4.5.4.2. Members making inappropriate CT calls are subject to disciplinary action even if the call does not cause additional expense. **Failure to observe the prohibitions and mandatory provisions of paragraph 4.5.4.2.1 by military personnel is a violation of the *Uniform Code of Military Justice (UCMJ)*, Article 92, Failure to Obey Order or Regulation. Violations by civilian employees may result in administrative disciplinary action without regard to otherwise applicable criminal or civil sanctions for violations of related laws. Violations by**

contactor personnel will be handled according to local laws and the terms of the contract.

4.5.4.2.1. Do not use Air Force issued CTs to conduct personal commercial activities. Some examples of inappropriate calls include those related to personal solicitation or sales matters and those of a harassing or obscene nature. If a caller has any questions concerning proper use of government cell phones, it is the caller's responsibility to check with a supervisor before making the call.

4.5.4.3. Dual line CTs. Individuals may elect at their option to activate the secondary line as a personal number and place personal calls on that line.

4.5.4.3.1. Activation of a dual-number capability is not permitted on secure CTs.

4.5.4.3.2. Authorized end user of a government-owned, dual-number capable CT:

4.5.4.3.2.1. Shall sign an agreement, produced in accordance with Base Judge Advocate and Contracting office guidance, that contains appropriate "hold harmless" and "personal liability" clauses, prior to being issued a dual-number capable CT, without regard to whether or not the user elects to immediately activate the secondary number capability.

4.5.4.3.2.2. If a secondary number is activated, the user must ensure all bills associated with the personal account are mailed directly to the user's home address or post office box.

4.5.4.3.2.3. When a CT is no longer required for the performance of duties, the user shall ensure that the personal account is closed and the secondary number zeroized by the vendor, prior to returning the CT to the local Personal Wireless Communications System (PWCS) manager for reuse.

4.6. **Official Telephone Service in Personal Quarters** is permitted for certain officials when necessary for national defense purposes. Contact your organizational TCO for more information, specific policy and procedures are contained in AFI 33-111, *Voice Systems Management*.

4.7. **Unofficial Commercial Telephone/Voice Service In Quarters.**

4.7.1. The individual subscriber must pay for renting, acquiring, and maintaining end-user instruments, as well as all usage charges for personal telephone service.

4.7.2. If required by the housing manager, housing occupants must restore telephone wiring and outlets to the original configuration before clearing quarters.

4.8. **Air Force Instruction on Defense Switched Network (DSN) On- or Off-Net Calling.**

4.8.1. Authorized Actions:

4.8.1.1. Placing an official call to a DSN operator (base operator) from a commercial network and having the operator extend the call over DSN to a DSN number (on-netting).

4.8.1.2. Placing an official call to a DSN operator from a DSN number and having the operator extend the call to a local commercial number (off-netting).

4.8.1.2.1. The installation CSO determines local guidance on the off-netting of an official DSN call to an official long-distance toll number. The installation CSO is directly responsible for toll charges and determines billing procedures, recourse for reimbursement, and/or acceptable appropriated fund support for off-netting official installation toll calls.

4.9. **Health, Morale, and Welfare (HMW) Calls.**

4.9.1. HMW calls are authorized over the DSN as prescribed in CJCSI 6215.01C, *Policy for Department of Defense Voice Networks with Real Time Services (RTS)*. HMW calls are not authorized on government-issued CT, or via the FTS-2001 (or its designated replacement) network. However, satellite phones may be approved for HMW calls by the Organizational Commander on a case-by-case basis. You can obtain copies of CJCS publications at **http://www.dtic.mil/doctrine/index.html**.

4.9.1.1. HMW calls are intended for military and Department of the Air Force civilians. HMW calls are authorized when:

4.9.1.1.1. In an unaccompanied status at overseas or remote geographic locations.

4.9.1.1.2. Single at overseas or remote geographic locations.

4.9.1.1.3. Performing extended temporary duty (TDY) for more than 14 days.

4.9.1.2. Immediate family members or the parents of single active duty personnel and/or the guardian of the child of a single parent or military/military couple, both of whom are deployed, may be permitted to participate in the HMW program under procedures established by the Airman and Family Readiness Center (i.e., as part of "Hearts Apart" or similar programs) and the host commander. It is both the deployed commander and the host base commander's responsibility to provide guidance on the limitations and opportunities made available by this program.

4.9.1.3. Place DSN HMW calls at routine precedence, normally not to exceed 15 minutes.

4.9.1.4. DSN HMW calls should not exceed a reasonable frequency as designated by the installation commander in conjunction with the installation CSO. Reasonable frequency is based upon installation/theater policy and determined by system capabilities, mission needs and restrictions. ***EXCEPTION:*** Emergency calls may exceed the established threshold.

4.9.1.5. Extending DSN HMW calls to a commercial number (off-netting) is authorized, provided it does not interfere with operational requirements. Off-net DSN HMW calls will not incur a toll charge to the government even if the intent is to reimburse the government. If the call incurs a toll charge, base operators may extend the call if the caller uses a credit/calling card to charge the call or the called party agrees to accept the charges (e.g., reversing of charges). See **paragraph 4.8.1.2.** for definition of off-netting.

4.9.1.6. On-netting of DSN HMW calls is permissible when placed from within the continental United States (CONUS) as part of Airman and Family Readiness "Hearts Apart" or other similar programs. See **paragraph 4.8.1.1.** for definition of on-netting.

4.10. **Emergency Service Calls.**

4.10.1. Dial 911 for all emergency services (e.g., police, fire, and medical emergencies) unless local guidance advises additional or alternate contact information for Emergency Services.

4.11. **Official Government Issued Calling Card Use.**

4.11.1. Government issued calling cards are issued for official use only. Cardholders must not use the calling card for any purpose other than official use. **Failure to observe the prohibitions and mandatory provisions of this paragraph by military personnel is a violation of the *Uniform Code of Military Justice (UCMJ)*, Article 92, Failure to Obey Order or Regulation. Violations by civilian employees may result in administrative disciplinary action without regard to otherwise applicable criminal or civil sanctions for violations of related laws. Violations by contactor personnel will be handled according to local laws and the terms of the contract.**

4.11.2. Cardholders must sign a statement acknowledging receiving the government issued calling card and that the card is for official use only.

5. Software.

5.1. **Government-owned Commercial Off-The-Shelf Software.** Do not install and use copies of government-owned software on a home computer unless the software license explicitly allows users to do so and the installation CSO has authorized such use. Personal use may be a violation of *The Copyright Act*, rendering the individual user accountable and liable. Reference AFI 51-303, *Intellectual Property--Patents, Patent Related Matters, Trademarks and Copyrights*.

5.2. Do not install software or hardware on an IS without coordination with the IAO. The IAO is responsible for the proper coordination and implementation through IA channels.

6. Electronic Messaging.

6.1. **General.** All government communications systems are subject to monitoring, interception, search, and seizure for all authorized purposes, reference DoD Chief Information Officer (CIO) Memorandum, *Policy on Use of Department of Defense (DoD) Information Systems Standard Consent Banner and User Agreement*, dated 9 May 2008. Government-provided messaging systems are for official or authorized purposes only. Any other use is prohibited.

6.1.1. Electronic messaging users will:

6.1.1.1. Maintain responsibility for the content of their electronic messages and ensure that messages sent meet Air Force acceptable use of electronic messaging (**paragraphs 6.2.**).

6.1.1.2. Maintain sent and received information according to Air Force records management directives: AFMAN 33-363; AFI 33-322, *Records Management Program*; and AFRIMS RDS (**https://afrims.amc.af.mil/rds_series.cfm**).

6.1.1.3. Adhere to local policy on sending electronic messages to a large number of recipients.

6.1.1.4. Adhere to local policy when sending an electronic message to mail distribution lists.

6.1.1.5. Only reply to electronic messages that absolutely require a response and minimize the use of the "Reply to All" function.

6.1.1.6. Bear sole responsibility for material accessed and sent.

6.1.1.7. Properly coordinate and staff electronic messages according to local directives.

6.1.1.8. Take appropriate action on non-delivery notices or message rejects to ensure messages reach the intended recipient.

6.1.1.9. Not auto-forward electronic messages from the ".mil" domain to a commercial Internet Service Provider (ISP).

6.1.1.10. Do not indiscriminately release electronic messaging addresses to the public. For further information, reference the Air Force Freedom of Information Act "Release of E-mail Addresses" (**http://www.foia.af.mil**).

6.1.1.11. Not add special backgrounds, special stationeries, digital images, unusual fonts, etc., to the body of their electronic messages.

6.1.2. Individual electronic messages are considered official when the sender is conducting mission-related or official business.

6.1.3. Special delivery instructions should be included as part of the message text to identify the specific addressee to whom the message is to be delivered. Type "FOR" followed by the name or position title when there is a specific person identified for delivery or "PASS TO" for address instructions to direct the message to a particular organization, unit, or office.

6.1.4. Messages with special delivery instructions should not be distributed through normal delivery channels unless specifically requested by the recipient.

6.1.5. Special Handling Requirements. Do not transmit controlled unclassified information (i.e. Privacy Act, FOUO) on or to systems not approved for that information. Reference AFI 31-401.

6.1.5.1. Transmitting unclassified information on classified networks is authorized unless specifically prohibited by the network operating instructions. The guidelines listed in **Attachment 2** apply to all unclassified electronic messages sent across a classified network.

6.1.5.2. Identify all Privacy Act and For Official Use Only (FOUO) electronic messages in the subject line with FOUO.

6.2. **Official Use, Authorized Use, and Use of Subscription Services.** Using Air Force messaging systems for other than official or authorized uses may result in adverse administrative or disciplinary action. **Failure to observe the prohibitions and mandatory provisions of 6.2.1.1.1. through 6.2.1.1.8. and 6.2.3.1. by military personnel is a violation of the *Uniform Code of Military Justice (UCMJ)*, Article 92, Failure to Obey Order or Regulation. Violations by civilian employees may result in administrative disciplinary**

action without regard to otherwise applicable criminal or civil sanctions for violations of related laws. Violations by contactor personnel will be handled according to local laws and the terms of the contract.

6.2.1. Official use includes communications, including emergency communications determined necessary in the interest of the Federal government. Official use includes, when approved by the theater commander in the interest of morale and welfare, those personal communications by military members and other Air Force employees who are deployed for extended periods away from home on official business.

6.2.1.1. The following do not constitute official use of government communications systems and are prohibited:

6.2.1.1.1. Distributing knowingly copyrighted materials by electronic messaging 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.

6.2.1.1.2. Sending or receiving electronic messages for commercial or personal financial gain.

6.2.1.1.3. Intentionally or unlawfully misrepresenting your identity or affiliation in electronic messaging communications.

6.2.1.1.4. Sending harassing, intimidating, abusive, or offensive material to, or about others.

6.2.1.1.5. Using someone else's identity (user identification [ID] name).

6.2.1.1.6. Causing congestion on the network by such things as the propagation of chain letters, junk E-mails, and broadcasting inappropriate messages to groups or individuals.

6.2.1.1.7. Using government systems for political lobbying.

6.2.1.1.8. Accessing commercial web mail accounts and instant messaging services (i.e., Yahoo, AOL, or MSN mail accounts).

6.2.1.2. Access to personal GI Mail and other instant messaging services on official Air Force web sites (i.e., AF Portal and AF Crossroads) is authorized since these services reside within the ".af.mil" domain and are specifically provided as a risk-mitigated alternative to their commercial counterparts. Wireless devices with web access are authorized to access official Air Force web mail services provided the devices are government issued and accountable.

6.2.2. Authorized Limited Personal Use Examples. Examples of authorized limited personal use include, but are not limited to:

6.2.2.1. Notifying family members of official transportation or schedule changes.

6.2.2.2. Using government systems to exchange important and time-sensitive information with a spouse or other family members (i.e., scheduling doctor, automobile, or home repair appointments, brief Internet searches, or sending directions to visiting relatives).

6.2.2.3. Educating or enhancing the professional skills of employees, (i.e., use of communication systems, work-related application training, etc.).

6.2.2.4. Sending messages on behalf of a chartered organization, (i.e., organizational Booster Club, Base Top 3, Base Company Grade Officers Association, etc.).

6.2.2.5. Limited use by deployed members for morale, health, and welfare purposes.

6.2.2.6. Job searching.

6.2.3. Use of Subscription Services. Internet electronic messaging access grants users the ability to subscribe to a variety of news, mail lists, and discussion groups. These services may include professional groups sponsored by Air Force agencies and other newsgroups sponsored by non-Air Force agencies, including the DoD, other Federal agencies, educational institutions, and commercial activities (i.e., product information updates and technical newsletters).

6.2.3.1. Air Force personnel may subscribe to official Air Force-sponsored news, mail lists, and discussion groups. Obtain written approval from the commander before subscribing to or participating in electronic message newsgroups except official Air Force internal information products. These products are managed and approved by SAF/PA and accessible from the Air Force Link (**http://www.af.mil**). Using such services without prior approval is misuse of a government system and is subject to disciplinary action, see **paragraph 6.2.** in this instruction. Subscription or participation in e-message news groups will be in support of official duties only.

6.2.3.2. When an extended absence will not allow access to your electronic messaging account, unsubscribe or suspend mail from any mail lists or newsgroups. This alleviates large backlogs of received messages that consume valuable server storage resources.

6.2.3.3. Participation in newsgroups whose content is contrary to the standards set by DoD 5500.7-R (i.e., obscene, offensive, etc.) is prohibited. Organizational commanders may direct electronic messaging administrators to set up permanent blocks on a specific site or newsgroup addresses to prevent subscription to such services.

6.3. **Electronic Message Signature Blocks.**

6.3.1. Electronic messages, to include official communications such as memorandums (letters), notes, messages, reports, etc., follow specific formats found in this instruction, Air Force Handbook (AFH) 33-337, *The Tongue and Quill*, AFI 33-321, *Authentication of Air Force Records,* and AFMAN 33-326, *Preparing Official Communications.*

6.3.1.1. Senders include a signature block on all official electronic messaging sent from individual or organizational accounts. Includes "//SIGNED//" in upper case before the signature block to signify it contains official Air Force information (e.g., instructions, directions, or policies). Restrict the signature block to name, rank, service affiliation, duty title, and phone numbers (DSN and/or commercial as appropriate) after the "//SIGNED//" entry, do not add slogans and quotes. Examples of appropriate signature blocks are in **Attachment 3**.

6.4. **Protecting Electronic Message Information.**

6.4.1. Controlled Unclassified Messages. There is information, other than classified information, that has been determined to require some type of protection or control.

6.4.1.1. Encrypt electronic messages when they contain controlled unclassified information, (i.e. Privacy Act, FOUO). See **paragraph 6.5.2.** for further information on encryption. See AFI 31-401 for additional guidance on controlled unclassified information.

6.4.1.2. Protecting FOUO Information. When transmitting FOUO information, add "FOUO" to the beginning of the subject line, followed by the subject. FOUO attachments shall be marked with a statement similar to this one: "FOR OFFICIAL USE ONLY ATTACHMENT." Additional protection methods may include password protecting the information in a separate Microsoft Word™ document. See AFI 31-401 for additional guidance on protecting FOUO information.

6.4.1.3. Protecting Personal Information. Transmitting personal information exempt under the Freedom of Information Act must be marked "FOUO" at the beginning of the subject line IAW guidance contained in AFI 31-401 and DoD 5200.1-R, *Information Security Program*, and apply the following statement at the beginning of the message:

"This email contains For Official Use Only (FOUO) information that may be exempt under the Freedom of Information Act, 5 United States Code (U.S.C.) 552."
Do not indiscriminately apply this statement to messages. Use it only in situations when you are actually transmitting personal information. Personal information may not be disclosed to anyone outside DoD unless specifically authorized by *The Privacy Act*.

6.4.1.3.1. Do not send Privacy Act information to distribution lists or group E-mail addresses unless each member has an official need to know the personal information.

6.4.1.4. Protecting Exempt *Freedom of Information Act (FOIA*) Information, Title 5, U.S.C., Section 552. Do not send FOIA information normally exempt in electronic messages without an appropriate level of protection to prevent unintentional or unauthorized disclosure. Refer to AFI 31-401 and DoD 5200.1-R for additional guidance or consult your local FOIA representative. Appropriate level of protection includes proper marking and encryption, see **paragraphs 6.4.1.2.** and **6.5.2.**

6.4.2. Classified Electronic Messages.

6.4.2.1. Marking Classified Electronic Messages. Mark all classified electronic messages with a level of classification equivalent to the information they contain or reveal.

6.4.2.1.1. Mark all electronic messages on classified networks by entering the appropriate classification in parenthesis by using these symbols: "(S)" for SECRET, "(C)" for CONFIDENTIAL, and "(U)" for UNCLASSIFIED, as the first marking in the "Subject" box of the message template. Following the subject, place the appropriate symbol indicating the appropriate classification of the subject itself. Do not send classified messages or mark messages as classified on an unclassified network.

6.4.2.1.2. Begin the text of the message on the third line (i.e., leave one blank line between the classification marking and the beginning of the message text).

6.4.2.1.3. Use the abbreviated classification symbol at the beginning of all paragraphs and subparagraphs.

6.4.2.1.4. Indicate the security classification of any attachments by placing the abbreviated classification symbol in parentheses before the attachment icon. If the message is unclassified without the attachments, then add this mandatory line: "THIS MESSAGE IS UNCLASSIFIED WHEN SEPARATE FROM ATTACHMENT."

6.4.2.1.5. Place Critical Nuclear Weapon Design Information, Cryptographic, Restricted Data, or other designators indicating special handling in the text following the security classification. Place markings for RESTRICTED DATA-ATOMIC ENERGY ACT 1954, and FORMERLY RESTRICTED DATA ATOMIC ENERGY ACT on the message as shown in DoD 5200.1-PH, *DoD Guide to Marking Classified Documents*; Air Force Policy Directive (AFPD) 31-4, *Information Security*; and AFI 31-401.

6.4.2.2. Message Declassification. Classified messages must contain declassification or downgrading instructions at the end of the message text. See AFI 31-401 for additional guidance.

6.4.2.3. Classified Electronic Message Destruction.

6.4.2.3.1. Destroy classified messages when no longer required. If the classified message is an official record, destroy it only after the retention period in AFRIMS RDS has expired.

6.4.2.3.2. TOP SECRET Control Officers use AF Form 143, *TOP SECRET Register Page*, or another approved form (e.g., AF Form 310, *Document Receipt and Destruction Certificate*) to record the destruction of TOP SECRET electronic messages.

6.4.2.3.3. When you must keep a record of destroyed SECRET and CONFIDENTIAL materials, use either AF Form 310 or AF Form 1565, *Entry, Receipt and Destruction Certificate*.

6.4.3. Message Destruction.

6.4.3.1. Protect messages from unauthorized or unintentional disclosure or destruction.

6.4.3.2. Users will destroy messages according to AFRIMS RDS instructions located at **https://afrims.amc.af.mil/rds_series.cfm**. Contact your CSA or ISO for proper destruction procedures.

6.5. **Digitally Signing and Encrypting Electronic Messages.**

6.5.1. Digitally Signing. Use PKI (Public Key Infrastructure) CAC digital signature certificates whenever it is necessary for the recipient of an electronic message to be assured of the sender's identity, have confidence the message has not been modified, or when non-repudiation is required. Messages containing only unofficial information and

not containing an embedded hyperlink and/or attachment should not be digitally signed. Refer to guidance in AFI 33-321 for policies concerning authenticating of e-mails. Contact your CSA for assistance. Examples of messages that should be digitally signed include:

6.5.1.1. Formal direction to a government employee or contractor.

6.5.1.2. Messages that stipulate an Air Force official position on any matter.

6.5.1.3. Messages that commit to, authorize, or deny the use of funds in some manner.

6.5.1.4. E-mails from user accounts and systems which contain an embedded hyperlink and/or attachment. Plain-text references to URL's do not require digital signature but they are recommended.

6.5.2. Encrypting. DoD PKI-based encryption is not authorized for protecting classified information on systems not approved for that use. Encryption increases bandwidth and resource requirements; therefore, e-mail encryption should be used to protect the following types of information, and the number of E-mail recipients should be kept to a minimum:

6.5.2.1. For Official Use Only (FOUO).

6.5.2.2. Privacy Act Information. For additional guidance see AFI 33-332.

6.5.2.3. Personally Identifiable Information (PII), (see Terms, **Attachment 1**).

6.5.2.4. Individually identifiable health, DoD payroll, finance, logistics, personnel management, proprietary, and foreign government information.

6.5.2.5. Contract data.

6.5.2.6. Export controlled technical data or information.

6.5.2.7. Operations Security (OPSEC) information. Encrypt critical information, OPSEC indicators, and other sources of information. For additional guidance on OPSEC requirements see AFI 10-701, *Operations Security*.

6.5.2.8. Information specified for encryption by domain owners pertaining to your individual areas of responsibility, see AFPD 33-4, *Enterprise Architecting*.

6.6. **Message Forwarding (Manual and Automated).** All previously stated guidance also applies to forwarded electronic messages. If the message was originally encrypted, it should not be forwarded outside the organization without being encrypted again. See **paragraph 6.4.2.1.** for further information on marking classified electronic messages.

6.6.1. Automated Message Forwarding.

6.6.1.1. Be aware that each message is automatically unsigned/unencrypted and distributed based on profiles loaded in the automated message distribution or profiling system.

6.6.1.2. Do not auto-forward official electronic messages to commercial Internet Service Providers (ISPs) from government computer systems.

6.6.1.3. Do not create automated message forwarding rules or procedures to send electronic messages to pagers, cell phones, commercial/non-military accounts.

6.7. **Message Management.** Electronic messages that are considered Air Force records IAW AFMAN 33-363 must be managed, stored, and deleted from the message system after copying to a record keeping system. If a digitally signed and/or encrypted official record is to be preserved, the user must follow procedures outlined in AFI 33-322. These procedures will ensure the information necessary to validate the digital signature is retained and the record is always accessible.

6.8. **Organizational Messaging** . Organizational messages are communications exchanged between organizational elements in support of command and control, combat support, combat service support, and other functional activities (defined by each functional community). Transmit organizational messages via the Defense Message System (DMS).

6.8.1. DMS is used for organizational messages that require a message release authority, are directive in nature, commit resources (i.e., forces to military action), make formal requests, or provide a command position.

6.8.2. Installation Commanders, Organization Commanders, and end users are responsible to ensure DMS is utilized when transmitting data or messages when the information being sent meets the definition of 'Organizational Message" as identified in **Attachment 1**.

6.8.3. Do not divulge Defense Message System (DSM) messages for other than official purposes to authorized personnel.

6.8.4. All DMS users will take the Automated Message Handling System (AMHS) training prior to being authorized access to any DMS-AF organizational account. Information for message handling instruction are covered in the AMHS computer based training (CBT). Contact your installation DMS Trusted Agent for access to the AMHS CBT.

7. Records Management. Records play a vital role in managing and operating Air Force activities. In simple terms, records document official business, serve as the memory of the organization, a record of past events, and are the basis for future actions. Every Air Force activity must manage its records to comply with legal accountability requirements. The key to an effective records management program is the integrity of the filing system--a system that ensures a standard methodology for filing, storing, retrieving, and ultimately disposing of records according to published retention and disposition schedules. AFMAN 33-363 establishes the requirement to use the Air Force Records Information Management System (AFRIMS); establishes guidelines for managing all records (regardless of media); and defines methods and the format for record storage, file procedures, converting paper records to other media or vice versa, and outlines the minimum to comply with records management legal and policy requirements.

7.1. Air Force Personnel, Civilian Employees, and Contractors:

7.1.1. Will receive annual government records management and PII training.

7.1.2. Must not conceal, remove, mutilate, obliterate or destroy government records without proper authority. Unauthorized concealment, removal, mutilation,

obliteration or destruction of records, or any attempt to do so, may be a violation of Title 18, U.S.C., Section 2071 and may be punished by up to three years confinement and a fine. **Violations by military personnel is a violation of the *Uniform Code of Military Justice (UCMJ),* Article 92, Failure to Obey Order or Regulation. Violations by civilian employees may result in administrative disciplinary action without regard to otherwise applicable criminal or civil sanctions for violations of related laws**. **Violations by contactor personnel will be handled according to local laws and the terms of the contract.**

7.1.3. Must inform officials of any actual or potential unlawful removal, change, or destruction of Air Force records.

7.1.4. Must distinguish government records from non-record materials and maintain personal papers separately. Contact your Records Custodian for assistance.

7.1.5. Encryption and Decryption. If encryption is used or if encrypted electronic messages are received, be aware of the periodic expiration of the certificates, currently every 3 years. Recommend users store electronic messages in the unencrypted form or plan to de-encrypt encrypted electronic messages prior to expiration of encryption certificate. Otherwise, when the encryption certificate is needed the user has to go through the key recovery process (through the appropriate CSA Help Desk) to gain the necessary keys to access encrypted electronic messages.

7.2. **Records Authentication.** The process used to ascertain the identity of a person or the integrity of specific record information. A record is authenticated when it contains an official signature or seal indicating the document is genuine and official. A signature or seal may be written, stamped, electronic or digital. Reference AFI 33-321.

8. Information Collection, Records, and Forms.

8.1. Information Collections. No information collections are created by this publication.

8.2. Records. The program records created as a result of the processes prescribed in this publication are maintained in accordance with AFMAN 33-363 and disposed of in accordance with the AFRIMS RDS located at **https://afrims.amc.af.mil/rds_series.cfm**.

8.3. Prescribed and Adopted Forms.

8.3.1. Adopted Forms:

AF Form 143, *TOP SECRET Register Page*;

AF Form 310, *Entry, Receipt and Destruction Certificate*;

AF Form 847, *Recommendation for Change of Publication*;

AF Form 1072, *Authorized Long Distance Telephone Calls*; and

AF Form 1565, *Entry, Receipt and Destruction Certificate*.

8.3.2. Prescribed Forms:

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

WILLIAM L. SHELTON,Lt General, USAF
Chief of Warfighting Integration and
Chief Information Officer

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

Title 5, U.S.C., Section 552a, as amended, *The Privacy Act of 1974*

Title 5, U.S.C., Section 552, *The Freedom of Information Act*

Title 44, U.S.C. § 3301, *Definition of Records*

Title 44 U.S.C. § 3542(B) (2)

DoD 5200.1-R, *Information Security Program*, 14 January 14 1997

DoD 5200.1-PH, *DoD Guide to Marking Classified Documents*, April 1997

DoD 5500.7-R, *Joint Ethics Regulation (JER)*, 1 August 1993 (Through Change 6, 23 March 2006)

DoDI 8500.2, *Information Assurance (IA) Implementation*, 6 February 2003

DoD Chief Information Officer (CIO) Memorandum, *Policy on Use of Department of Defense (DoD) Information Systems Standard Consent Banner and User Agreement*, 9 May 2008, **http://iase.disa.mil/policy-guidance/dod-banner-9may2008-ocr.pdf**

CJCSI 6215.01C, *Policy for Department of Defense Voice Networks with Real Time Services (RTS)*, 9 November 2007

AFI 10-701, *Operations Security*, 18 Oct 2007

AFI 10-901, *Lead Operating Command--Communications and Information Systems Management*, 22 March 2001

AFPD 13-3, *Air Force Network Operations (AFNetOps)*, 11 January 2008

AFPD 31-4, *Information Security*, 1 September 1998

AFI 31-401, *Information Security Program Management*, 1 November 2005

AFI 33-106, *Managing High Frequency Radios, Personal Wireless Communication Systems, And The Military Affiliate Radio System*, 13 February 2007

AFI 33-111, *Voice Systems Management*, 5 November 2007

AFI 33-119, *Air Force Messaging*, 18 May 2007

AFI 33-129, *Web Management and Internet Use*, 3 February 2005

AFI 33-200, *User Responsibilities and Guidance for Information Systems*

AFI 33-202, Volume 6, *Identity Management*, 23 May 2005 (will become AFSSI 8520, *Identification and Authentication*)

AFI 33-321, *Authentication of Air Force Records*, 27 July 2006

AFI 33-322, *Records Management Program*, 7 October 2003

AFI 33-332, *Privacy Act Program*, 29 January 2004

AFI 36-3026(I), *Identification Cards for Members of the Uniformed Services, Their Eligible Family Members, and Other Eligible Personnel*, 20 December 2002

AFI 31-501, *Personnel Security Management Program*, 27 January 2005

AFI 51-303, *Intellectual Property--Patents, Patent Related Matters, Trademarks and Copyrights*, 1 September 1998

AFJI 31-102, *Physical Security*, 31 May 1991

AFMAN 33-326, *Preparing Official Communications*, 15 October 2007

AFMAN 33-363, *Management of Records*, 3 March 2008

AFH 33-337, *The Tongue and Quill*, 1 August 2004

AFPD 33-1, *Information Resources Management*, 27 June 2006

AFPD 33-2, *Information Assurance (IA) Program*, 19 April 2007

AFPD 33-4, *Enterprise Architecting*, 27 June 2006

Abbreviations and Acronyms

AFCA—Headquarters, Air Force Communications Agency

AFH—Air Force Handbook

AFI—Air Force Instruction

AFMAN—Air Force Manual

AFRIMS—Air Force Records Information Management System

C2—Command and Control

C4ISR—Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance

CAC—Common Access Card

CBT—Computer-Based Training

CIPS—C4ISR Infrastructure Planning System

CJCSI—Chairman of the Joint Chiefs of Staff Instruction

COMSEC—Communications Security

CONUS—Continental United States

CSA—Client Support Administrator

CSO—Communications and Information Systems Officer

CT—Cellular Telephone

CUI—Controlled Unclassified Information

DAA—Designated Accrediting Authority

DISA—Defense Information Systems Agency

DMS—Defense Message System

DoD—Department of Defense

DoDI—Department of Defense Instruction

DSN—Defense Switched Network

Email—Electronic Mail

EMSEC—Emission Security

FOIA—Freedom of Information Act

FOUO—For Official Use Only

GIG—Global Information Grid

HMW—Health, Morale, and Welfare

IA—Information Assurance

IAO—Information Assurance Officer

ID—Identification

IT—Information Technology

MAJCOM—Major Command

OMB—Office of Management and Budget

OPSEC—Operation Security

PED—Portable Electronic Device

PDA—Personal Digital Assistants

PII—Personally Identifiable Information

PIN—Personal Identification Number

PKI—Public Key Infrastructure

PWCS—Personal Wireless Communications System

RDS—Records Disposition Schedule

SAF—Secretary of the Air Force

STEM—Systems Telecommunications Engineering Manager

STEM-B——STEM-Base Level

STEM-C——STEM-Command Level

STEM-D——STEM-Deployability

STEM-J——STEM-Joint

STEM-TM——STEM-Telecommunications Manager

TCO—Telephone Control Officer

TDY—Temporary Duty

UCMJ—Uniform Code of Military Justice

US—United States

US&P—United States and Possessions

USAF—United States Air Force

USB—Universal Serial Bus

User-ID—User Identification

Terms

Accountable Officer—An individual appointed by proper authority who maintains item records and/or financial records in connection with Government property, irrespective of whether the property is in his or her possession for use or storage, or is in the possession of others to whom it has been officially entrusted for use or for care and safekeeping. (AFI 33-112)

Air Force-Global Information Grid (AF-GIG)—The Air Force-provisioned portion of the Global Information Grid (GIG) that the Air Force has primary responsibility for the procurement, operations, and defense. It provides global connectivity and services, in addition to C2 of that connectivity and those services that enable Air Force commanders to achieve information and decision superiority in support of Air Force mission objectives. The AF-GIG consists of fixed, mobile, and deployable facilities, and equipment, as well as processes, trained personnel and information. (AFPD 13-3)

Base-Level Communications and Information Infrastructure—Both host and tenant organizations use the base-level communications and information systems infrastructure. The infrastructure includes all aspects of communications and information systems (voice, data, video transmission, switching, processing, system control and network management systems, equipment, and facilities). (AFI 33-103)

Common Access Card (CAC)—CAC is the DoD identification card. It is a credit card-sized ID card that contains integrated circuit chips, a magnetic strip, bar codes, and a photo. The integrated circuit chip is where the certificates/keys reside. In addition to being the DoD identification card, the CAC is used to digitally sign e-mail, travel orders, travel vouchers and other documents, and establish secure web-based sessions. (AFMAN 33-223, will become AFSSI 8520)

Client Support Administrator (CSA) (will become Client Support)—CSAs support customers with resolving issues relating to information technology devices, such as personal computers, personal digital assistants, and printers.

Communications and Information System—An integrated combination of doctrine, procedures, organizational structures, personnel, equipment, communications-electronics equipment and systems, facilities, and communications designed to support a commander's exercise of command and control through all operational phases. It includes base visual information support systems. (AFI 33-103)

Communications and Information Systems Officer (CSO)—The designated official who has overall responsibility for communications and information support at any given level of the Air

Force (base, tenant, MAJCOM, USAF, etc.). At base level, this is the commander of the communications unit responsible for carrying out base communications and information systems responsibilities. At MAJCOM and other activities responsible for large quantities of communications and information systems, it is the person designated by the commander as responsible for overall management of communications and information systems budgeted and funded by the MAJCOM or activity. CSOs are the accountable officer for all automated data processing equipment in their inventory and are responsible for maintenance of the communications blueprint through the use of the C4ISR Infrastructure Planning System (CIPS). (AFI 33-103)

Communications and Information Systems Requirement—Either a document that identifies a C&I systems mission shortfall or system need to the CSO. A C&I systems requirement arises when an organization cannot accomplish its current or new mission; can increase operational efficiency or cut operational costs by using advances in technologies; or can modernize an existing IS by applying modern technology to satisfy evolving requirements, improve mission performance, and reduce current or future operation and support costs. The process starts when the user identifies a required capability and requests CSO assistance with defining the requirement and developing a technical solution for that need. The CSO must involve the Systems Telecommunications Engineering Manager (STEM), the lead command, frequency management, communications security (COMSEC) activities, and others to develop the technical solution and will use the requirements process within C4ISR Infrastructure Planning System (CIPS), to submit and process requirements. The CSO will provide assistance with implementing the technical solution. (AFI 33-103)

Controlled Unclassified Information (CUI)—Unclassified information to which access or distribution limitations have been applied in accordance with national laws, policies, and regulations of the originating country. It includes United States (US) information that is determined to be exempt from public disclosure or that is subject to export controls in accordance with the international traffic in arms regulations or the export administration regulations. AFI 31-401 provides specific guidance on proper handling of CUI.

Designated Accrediting Authority (DAA)—Official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. Synonymous with Designated Approving Authority and Delegated Accrediting Authority. (AFPD 33-2)

Domain—A functional area of responsibility. (AFPD 33-4)

Emission Security (EMSEC)—The protection resulting from all measures taken to deny unauthorized personnel information of value that might be derived from communications systems and cryptographic equipment intercepts and the interception and analysis of compromising emanations from cryptographic-equipment, information systems, and telecommunications systems. (AFI 33-200)

Emission Security (EMSEC) Manager—The designated person responsible for the management of EMSEC; usually part of Wing IA Office. (AFSSI 7700, 24 October 2007)

Global Information Grid (GIG)—The globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and

services, software (including applications), data, security services, and other associated services necessary to achieve Information Superiority. It also includes National Security Systems as defined in section 3542(B)(2) of Title 44 United States Code (U.S.C.). The GIG supports all DoD, National Security, and related Intelligence Community missions and functions (strategic, operational, tactical, and business), in war and in peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms, and deployed sites). The GIG provides interfaces to coalition, allied, and non-DoD users and systems. It includes any system, equipment, software, or service that meets one or more of the following criteria: transmits information to, receives information from, routes information among, or interchanges information among other equipment, software, and services; provides retention, organization, visualization, information assurance, or disposition of data, information, and/or knowledge received from or transmitted to other equipment, software, and services; processes data or information for use by other equipment, software, or services. (AFPD 13-3)

Information Assurance Officer (IAO)—IAOs are assigned to each organization by the organization commander or other cognizant authority (i.e., group-level commander, Wing IA office) when IA functions are consolidated to a central location or activity. Additional (subordinate) IAO positions may be assigned for additional support at the discretion of organizations or based upon mission requirements. (AFI 33-202V1, will become AFI 33-200)

Information System (IS)—Set of information resources organized for collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Includes automated information system (AIS) applications, enclaves, outsourced IT-based processes, and platform IT interconnections. (AFI 33-202V1, will become AFI 33-200)

Information System Owner (ISO)—Ultimate recipient of the IS. Official responsible for the oversight of the procurement, development, integration, modification, and operation and maintenance of an IS. Informs key officials of the need to conduct a security certification and accreditation of the system, ensures appropriate resources are available for the effort, and provides necessary system-related documentation to the CA. Submits certification and accreditation package to the Certification Authority's Representative for validation and recommendations, and then to the DAA's designated representative for adjudication. (AFPD 33-2)

Information Technology (IT)—Any equipment, or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. This includes equipment used by a Component directly, or used by a contractor under a contract with the Component, which (i) requires the use of such equipment, or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term "IT" also includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. Notwithstanding the above, the term "IT" does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract. The term "IT" includes National Security Systems (NSS). (AFPD 33-2)

Lead Command—The MAJCOM or field operating agency assigned as systems advocate and oversight authority for communications and information systems used by more than one command. Specific responsibilities of the lead command are in AFI 10-901.

Modification—A temporary or permanent change to a system that is still being produced. The purpose of the modification is to correct deficiencies, improve reliability and maintainability, or to improve capabilities. (AFI 33-103)

Non-Record Materials—U.S. Government-owned documentary materials excluded from the legal definition of records or not meeting the requirements of that definition. Include extra copies of documents kept only for convenience of reference, stocks of publications and of processed documents, and library or museum materials intended solely for reference or exhibition; also called non-record copies or non-records. (See Title 44 United States Code [U.S.C.] 3301)

Organizational Message—Includes messages and other communications exchanged between organizational elements in support of command and control, combat support, combat service support, and other functional activities. These messages provide formal direction or establish a formal position, commitment, or response for the organization. Organizational messages require approval for transmission by designated officials of the sending organization and determination of internal distribution by the receiving organization. Because of their official and sometimes critical nature, organizational messages impose operational requirements on the communications system for capabilities such as precedence, timely delivery, and high availability and reliability. (AFI 33-113)

Personal Digital Assistant (PDA)—Hybrid handheld automated data processing equipment (e.g., Palm Pilot®, Cassiopeia® or BlackBerry™) that are designed for use as multi-functional voice and/or data wireless communications-computer devices.

Personally Identifiable Information (PII)—Any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual. For DoD information assurance purposes, electronic PII records are categorized according to the potential negative impact of loss or unauthorized disclosure according to FIPS Pub 199. (AFI 33-200)

Personally Identifiable Information (PII) Category—For DoD information assurance purposes, consistent with OMB M-06-16, "Protection of Sensitive Agency Information," 23 June 2006 and FIPS 199, electronic PII records are categorized according to the potential negative impact of loss or unauthorized disclosure:

High Impact. Any Defense-wide, organizational (e.g., unit or office), program or project level compilation of electronic records containing PII on 500 or more individuals stored on a single device or accessible through a single application or service, whether or not the compilation is subject to The Privacy Act. Also, any compilation of electronic records containing PII on less than 500 individuals identified by the Information or Data Owner as requiring additional protection measures. Examples: A single mobile computing or storage device containing PII on 500 or more individuals, even if the PII is distributed across multiple files or directories, is considered High Impact PII. A DoD enclave of 500 or more users, with the PII for each user embedded in his/her individual workstation, is not considered High Impact PII.

Moderate Impact. Any electronic records containing PII not identified as High Impact. (AFI 33-200)

Personal Wireless Communications System (PWCS)—A user centric service that is accessible via devices either vehicular mobile, hand carried, or worn by individual users. Each user may have an individually identifiable electronic address. (AFI 33-106)

Portable Electronic Device (PED)—Any non-stationary electronic apparatus with the capability of recording, storing, and/or transmitting information. This definition includes, but is not limited to PDAs, cellular/PCS phones, two-way pagers, email devices, audio/video recording devices, and hand-held/laptop computers. (AFI 33-200)

Protected Workplace—Workplaces that minimally satisfy Physical and Environmental Controls for Confidentiality Level Sensitive as established in DoDI 8500.2., AFJI 31-102, and AFI 31-401 provide additional guidance for physical and information security, respectively. (AFI 33-200)

Public Key Infrastructure—PKI is a service of products which provide and manage X.509 certificates for public key cryptography. Certificates identify the individual named in the certificate, and bind that person to a particular public/private key pair. DoD PKI provides the data integrity, user identification and authentication, user non-repudiation, data confidentiality, encryption and digital signature services for programs and application, which use the DoD networks. (AFI 33-202, Volume 6, will become AFSSI 8520)

Records— "All books, papers, maps, photographs, machine readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the US Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of data in them. Library and museum material made or acquired and preserved solely for reference or exhibition purposes, extra copies of documents preserved only for convenience of reference, and stocks of publications and of processed documents are not included." May also be called Federal records that exclude Presidential records and records of the U.S. Congress. (AFI 33-322)

Records Custodian—The individual responsible for physical custody, maintenance, and disposition of records accumulated in the performance of a particular function. The directorate/separate office/activity records officer designates the files custodian in designating the directorate "office of record." Depending upon the size and complexity of the directorate, the RM may elect to designate more than one office of record/files custodian for the records it holds. (AFI 33-322)

Requirements Process—This three-step process identifies communications and information systems requirements, develops a technical solution, and allocates resources. (AFI 33-103)

Sensitive Information—Information, the loss, misuse, or unauthorized access to, or modification of, which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under 5 United States Code Section 552a (The Privacy Act), but that has not been specifically authorized under criteria established by Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. (Systems that are not national security systems, but contain sensitive information are to be protected in accordance with the requirement of the Computer Security Act of 1987 [P.L. 100-235].)

Telephone Control Officer (TCO)—Individual who authorizes and controls long distance telephone toll calls within a unit.

Username or User Identification (user-ID)—Unique symbol or character string used by an information system to identify a specific user.

User—All users who use or have access to a government Information System and government computer devices, to include government desktop and laptop computers, mobile devices and email systems.

Table A1.1. World Wide Web (WWW) Sources:

Referenced	URL	Topic	Organization	Web Page POC
Accessibility	http://www.e-publishing.af.mil	Air Force Publishing	AFDPO	e-publishing@pentagon.af.mil
Purpose Statement	https://afrims.amc.af.mil/rds_series.cfm	Air Force Records Disposition Schedule	AFCA/EAL	Web Master: afca.rims@scott.af.mil
Paragraph 4.9.1.	http://www.dtic.mil/doctrine/index.html	Joint Electronic Library	DTIC	Web Master: bcporder@dtic.mil
Paragraph 6.1.1.10	http://www.foia.af.mil	Air Force Freedom of Information Act	Air Force Freedom of Information, Privacy Act and Quality of Information Office	(703) 696-6515
Paragraph 6.2.3.1.	http://www.af.mil	Electronic Message Newsgroup	SECAF/PA	Web Master: Not Available
Attachment 1	http://iase.disa.mil/policy-guidance/dod-banner-9may2008-ocr.pdf	Information Assurance Support Environment	DISA	Web Master: IA-web@disa.mil

Attachment 2

TRANSMITTING UNCLASSIFIED INFORMATION ON CLASSIFIED NETWORKS

A2.1. Transmitting Unclassified Information on Classified Networks. Use the following guidelines for all unclassified messages sent across any network cleared for classified material.

A2.1.1. Mark unclassified electronic messaging messages sent across classified networks by entering the symbol "(U)" in parenthesis as the first marking in the "Subject" box of the message.

A2.1.2. Identify any special messaging handling requirements (i.e., "Pass To" and "For").

A2.1.3. Identify the "From" (message originator) and "To" (message recipients) addresses.

A2.1.4. Begin the text of the message after all required administrative information identified in **paragraph A2.1.1.** through **A2.1.5.**

A2.1.5. Attachments included in an unclassified message transmission do not need to have the classification noted. ***Note:*** If an attachment is classified, the entire electronic messaging transmission is classified.

Attachment 3

ELECTRONIC MESSAGE SIGNATURE BLOCK EXAMPLES

A3.1. Military Signature Block:

A3.1.1. Active Duty:

//SIGNED//
RAINY DAYS, Maj, USAF
Branch Chief, Messaging Services
DSN 555-5555 Comm (555)555-5555

A3.1.2. Military Reservist:

//SIGNED//
Robert Osprey, Lt Col, USAFR
Branch Chief, Employee Services
DSN 555-5555 Comm (555)555-5555

A3.1.3. National Guard:

//SIGNED//
Joseph A. Chinook, SMSgt, NG
Superintendent, Life Skills
DSN 555-5555 Comm (555)555-5555

A3.1.4. Active Duty Coast Guard:

//SIGNED//
Harold S. Skywarrior, CWO, CG
OIC, Transportation Flight
DSN 555-5555 Comm (555)555-5555

A3.2. DoD Civilian Signature Block:

//SIGNED//
Raptor Dominance, GS-12, DAF
Branch Chief, Field Support
DSN 555-5555 Comm (555)555-5555

A3.3. Contractor Signature Block:

//SIGNED//
Kitty Hawk, Contractor, HQ AFCA/ECFP
DSN 555-5555 Comm (555)555-5555

Attachment 4

PASSWORD MANAGEMENT QUICK REFERENCE SHEET

A4.1. The DOs of Password Management. Do:

A4.1.1. Use a combination of letters (upper and lower case), numbers, and special characters. Password must include at least two of each character type.

A4.1.2. Use a length of nine or more characters in the password.

A4.1.3. Change your password every 60 days.

A4.1.4. Enter the password carefully making sure nobody is watching.

A4.1.5. Use your account regularly to help you remember your password.

A4.1.6. Contact your ISSO if you suspect your password has been compromised.

A4.1.7. Ensure your password is not exposed on the screen during login.

A4.1.8. Verify the login information provided to ensure your account has not been used since your last session.

A4.2. The DO NOTs of Password Management. Do not:

A4.2.1. Use a single word by itself for the password; especially ones from the dictionary, slang words, names, or profanity.

A4.2.2. Use words personally associated with you.

A4.2.3. Write down your password unless absolutely necessary; if written, protect it so you are the only one who knows it.

A4.2.4. Store your password on the desk, wall, terminal or in a function key or the communications software.

A4.2.5. Share your password with anyone.

A4.2.6. Let anyone watch you enter your password.

A4.2.7. Leave your terminal unprotected while you are logged in.

Attachment 5

LISTING OF PUBLICATIONS THAT USER POLICY C&I INFORMATION WAS EXTRACTED FROM

A5.1. AFI 33-106, *Managing High Frequency Radios, Personal Wireless Communication Systems, And The Military Affiliate Radio System*, 13 Feb 2007.

A5.1.1. Deleted **Paragraphs 4.9.1.1.**, **4.9.3.1.** through **4.9.3.2.2.**, **4.9.3.4.**, **4.9.3.6.**, **4.9.3.7.**, **4.9.4.3.**, **4.9.4.4.**, **4.9.4.6.** through **4.9.4.7.**, **4.9.6.**

A5.1.2. Amended **Paragraphs 4.9.3.3.**; **4.9.3.5.**, **4.9.4.**, **4.9.4.5.**, **4.9.5.**; **4.10.**

A5.2. AFI 33-111, *Voice Systems Management*, 24 Mar 2005.

A5.2.1. Deleted **Paragraphs 13.1.**, **13.3.**, **13.4.**, **14.-15.5.**, **17.3.**, **20.1.** through **20.3.**, **30.1.3.**, **30.1.5.**, **39.1.1.** through **39.1.2.1.**, **40.1.** through **40.6.**

A5.2.2. Amended **Paragraph 40.**

A5.3. AFI 33-114, *Software Management*, 13 May 2004.

A5.3.1. Deleted **Paragraphs 8.** through **8.3.**

A5.4. AFI 33-115, Volume 2, *Licensing Network Users and Certifying Network Professionals*, 14 Apr 2004.

A5.4.1. Amended **Paragraphs 5.3.**; **5.4.**

A5.5. AFI 33-119, *Air Force Messaging*, 24 Jan 2005.

A5.5.1. Deleted **Paragraphs 1.8.7.**, **1.8.10.**; **3.**, **3.3.** through **3.5.**, **3.9.** through **3.9.1.2.**, **3.9.3.** through **3.10.**, **3.10.2.**, **3.10.2.1.**, **3.10.2.3.**, **3.12.**, **3.14.**, **4.** through **4.2.3.**, **6.1.** through **6.1.1.3.**, **6.1.2.1.** through **6.1.2.7.**, **7.1.**, **7.2.1.**, **8.4.2.**, **8.4.4.**, **8.4.5.**, **8.6.** through **8.8.3.**, **8.9.**, **8.9.2.**, **8.9.3.**

A5.5.2. Deleted **Attachments 3** and **4**.

A5.5.3. Amended **Paragraphs 3.7.**, **3.10.2.4.**, **3.13.**, **7.2.2.**, **6.1.2.**, **8.4.3.**, **7.2.2.**

A5.6. AFI 33-129, *Web Management and Internet Use*, 03 Feb 2005.

A5.6.1. Deleted **Paragraphs 2.1.** through **2.2.14.**

A5.7. AFMAN 33-223, *Identification and Authentication*, 29 Jul 2005.

A5.7.1. Deleted **Paragraphs 3.4.1.**, **4.2.1.** through **4.2.3.**, and **Attachment 2.**

A5.7.2. Amended **Paragraph 4.3.**

A5.8. The following publications are being rescinded:

A5.8.1. AFI 33-202, Volume 1, *Network and Computer Security*, 18 May 2007.

A5.8.2. AFI 33-202, Volume 6, *Identity Management*, 23 May 2005.