BY ORDER OF THE COMANDER
939 AIR REFUELING WING (AFRC)

939 AIR REFUELING WING
INSTRUCTION 33-201

1 APRIL 2003

Communications and Information

COMMUNICATION AND COMPUTER MANAGEMENT AND SECURITY

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

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

OPR: 939 CF/SCBN (Mr David P. Craig)
Supersedes 939 RQWI 33-201, 5 July 2002

Certified by: 939 MSG/CC (Col Richard A. Gano)
Pages: 33
Distribution: F

This instruction implements AFPD 33-1, *Command, Control, Communications, and Computer (C4) Systems* and AFPD 33-2, *Information Protection*. This instruction provides policy for use of the 939 ARW Local Area Network (LAN) (e.g. E-mail use, Internet/Intranet use, and use of other associated systems utilizing the 939 ARW LAN); 939 ARW points of contact (POC), connection to 939 ARW LAN, software use and licensing issues, classified processing, and security incident reporting, web page creation and maintenance, malicious logic, C4 management and use and other related issues. This instruction directs the use of PIA Form 33-115, *Worksheet and Network System Access*. This instruction applies to all activities supported by the 939 Air Refueling Wing LAN, Portland IAP, OR.

SUMMARY OF REVISIONS

This document is substantially revised and must be completely reviewed.

This revision changes unit designation from 939th Rescue Wing to 939th Air Refueling Wing. It also incorporated the Information Usage and Management Policy letter dated 5 Oct 02. It updates section **2.6.**, Website Management, with updated information and procedures to add web pages to the wing intranet web site.

Chapter 1

GENERAL INFORMATION

1.1. PURPOSE. The purpose of this instruction is to standardize many processes used to administer, protect, and manage 939 ARW Portland ANGB, OR LAN. As the LAN becomes an increasingly integral part of the day-to-day functions of the 939 ARW, it is necessary for users to know and understand the rules of engagement for proper and secure use of its information net services, automated data processing equipment (ADPE) and software.

1.2. 939 ARW LAN DESCRIPTION. 939 ARW LAN is a sensitive but unclassified (SBU) LAN. It provides office automation, print services, E-mail services, and Inter/Intranet services.

1.3. RESPONSIBILITIES.

1.3.1. 939 ARW Designated Approval Authority (DAA) is the wing commander. The DAA will:

1.3.1.1. Approve the certification and accreditation (C &A) package of the 939 ARW LAN.

1.3.1.2. Approve all hardware and software to operate on the 939 ARW LAN.

1.3.1.3. Approve all personal hardware or software to operate on or with government equipment.

1.3.1.4. Approve the use of government equipment, hardware and software, for other than Official Use as outlined in AFI 33-112, *Computer Systems Managemen*t.

1.3.2. 939 ARW Organizational Commanders will:

1.3.2.1. Ensure applicable instructions are followed by members within their organization.

1.3.2.2. Notify the 939 ARW Computer Security Officer (CSO) and 939 CF/SCBI of any and all inappropriate internet and computing activities.

1.3.2.3. Ensure system administrators (SA), workgroup managers (WM), information systems security officer (ISSO), terminal area security officer (TASO), telephone control monitors (TCM), equipment custodians (EC) and web page maintainers (WPM) are appointed. Appointments will be documented by memorandum to the 939 ARW CSO.

1.3.3. 939 ARW CSO will:

1.3.3.1. Ensure security policies and practices are in place and disseminated to all 939 ARW LAN operations personnel, 939 ARW LAN points of contact (POC), and users.

1.3.3.2. Ensure all network account requests are coordinated with the individual's supervisor; mandatory IA briefing and training are accomplished prior to assigning an account; and security clearance information is verified on the requestor.

1.3.3.3. Review computer logs on ADPE to ensure compliance with AFI 33-129, *Transmission of Information via the Internet,* based on reported incidents from 939 ARW LAN users and through group commander's request.

1.3.3.4. Ensure maintenance and 939 ARW LAN users are aware of this instruction through 939 ARW LAN POC.

1.3.4. 939 ARW LAN Manager (939 CF/SCBN) will:

1.3.4.1. Ensure network security policies and practices are complied with on all 939 ARW LAN components.

1.3.4.2. Ensure current accreditation of 939 ARW LAN and verify accreditation of systems connected to 939 ARW LAN.

1.3.4.3. Be familiar with applicable references and ensure compliance with applicable instructions.

1.3.4.4. Ensure maintenance and mandatory backups of 939 ARW LAN components are completed and performed on schedule.

1.3.4.5. Ensure all required firmware and software upgrades are performed and reported through the CSO.

1.3.4.6. Ensure all higher headquarters, host base and AFCERT Advisories and Compliance Messages are responded to through the 939 ARW CSO for inclusion to the required reporting procedures.

1.3.4.7. Ensure all network account requests coordinated with the individual's supervisor; that the mandatory information assurance (IA) briefing and training are accomplished prior to assigning an account and that security clearance information is verified on the requestor.

1.3.4.8. Chair the 939 ARW Communications and Computer Working Group (C2WG) meetings.

1.3.5. Work group managers(WM)

1.3.5.1. Will act in the following capacity (may require internal monitors to assist): group ISSO, TASO, and EC. Basic responsibilities for these positions are described in 33 and AFSSI 5000 series instructions.

1.3.5.2. Ensure all AFCERT messages are complied with and responded to in the required timeframe.

1.3.5.3. Ensure all network account requests are requested through the individual's supervisor; that the mandatory IA briefing and training are accomplished prior to assigning an account ; and that security clearance information is verified on the requestor.

1.3.5.4. Act as liaison between 939 ARW LAN and their respective area(s). They are to ensure user awareness of established directives, in this instruction and other 939 ARW LAN supplied policies and procedures. WMs must also maintain a working relationship with the wing information assurance office (IAO).

1.3.5.5. Oversee assignment of web providers; assign permissions for specific web pages.

1.3.5.6. Attend 939 ARW C2WG meetings or send a representative.

1.3.5.7. Be familiar with software licensing rules and ensure 939 ARW LAN users in their area are familiar with licensing rules as they pertain to 939 ARW LAN.

1.3.5.8. Be aware of and ensure user awareness of virus reporting procedures contained in **Chapter 4** of this instruction..

1.3.6. System administrators (SA) will:

1.3.6.1. Ensure all AFCERT messages are complied with and responded to in the required time-frame.

1.3.6.2. Ensure all network account requests are coordinated with the individual's supervisor; that the mandatory IA briefing and training are accomplished, and given to the WM for action.

1.3.6.3. Act as liaison between 939 ARW LAN and their respective area(s). They are to ensure user awareness of established directives, in this instruction and other 939 ARW LAN supplied policies and procedures. SAs must also maintain a working relationship with the wing IAO.

1.3.6.4. Attend 939 ARW C2WG meetings or send a representative.

1.3.6.5. Be familiar with software licensing rules and ensure 939 ARW LAN users in their area(s) are familiar with licensing rules as they pertain to 939 ARW LAN.

1.3.6.6. Be aware of and ensure user awareness of virus reporting procedures contained in this instruction.

1.3.7. Web administrator (WA) will:

1.3.7.1. Ensure all AFCERT messages are complied with and responded to in the required time-frame.

1.3.7.2. Oversee the 939 ARW Intranet web sites for compliance with applicable directives.

1.3.7.3. Oversee the assignment of web providers; assign permissions for specific web pages.

1.3.7.4. Maintain and keep current the 939 ARW Intranet main web page and disclaimer page.

1.3.7.5. Act as liaison between 939 ARW LAN and web page providers. Ensure user awareness of established directives and 939 ARW LAN supplied policies and procedures. WAs must also maintain a working relationship with the wing IAO.

1.3.7.6. Attend 939 ARW C2WG meetings or send a representative.

1.3.7.7. Be aware of and ensure user awareness of virus reporting procedures contained in **Chapter 4** of this instruction.

1.3.8. Some of these positions have additional responsibilities outlined within the context of this instruction.

Chapter 2

REQUIREMENTS

2.1. SYSTEM MANAGEMENT AND SECURITY PLAN (SMSP). All 939 ARW LAN users with access to 939 ARW LAN resources must be familiar with applicable procedures in this instruction. Failing to adhere to this instruction is grounds for denial of service by 939 ARW LAN personnel and may be grounds for administrative or disciplinary action against individuals involved. The CSO will ensure this instruction is available to all affected personnel via 939 ARW LAN's intranet or other publicized means.

2.2. NOTICE AND CONSENT FOR TELECOMMUNICATIONS MONITORING. General notification is hereby given to users of DoD telecommunications systems or devices DoD provides such systems and devices for conducting official government business. Use of government telecommunications systems and devices constitutes consent by the user to telecommunications monitoring. See AFI33-219, *Telecommunications Monitoring and Assessment Program (TMAP*).

2.3. CONTINGENCY PLANNING.

2.3.1. Contingency Planning Requirement. All 939 ARW units using the 939 ARW LAN are responsible for creating, coordinating, and maintaining their contingency plans in the event of an extended 939 ARW LAN outage. Plans should be coordinated through your unit WM, the wing CSO, and wing plans to ensure feasibility and licensing commitments are met.

2.3.2. Data Storage on 939 ARW LAN and Backup. In addition to basic administrative support considerations (e.g., word processing, E-mail, etc.), 939 ARW units must evaluate and document their data stored on 939 ARW LAN servers and implement backup procedures based on the impact of loss of access to 939 ARW LAN by identifying the criticality and currency of the data. When possible, backups should be performed to media other than that of the 939 ARW LAN (i.e., user's hard drive, tape backup in user's work center, user's floppy disk, etc.).

2.3.3. Directed by the Joint Chiefs of Staff, the information threatcon (INFOCON) system presents a structured coordinated approach to react to and defend against adversarial attacks on DoD computers, telecommunications and networks. Information protection is protection to preserve the availability, integrity, and confidentiality of the systems and the information contained within the systems. Incorporating information protection is an integral part of all planning. The wing point of contact for all INFOCON actions is the 939 ARW LAN Manager. The 939 ARW must abide by the direction from our higher headquarters and our host IA authority on specific threats known to our installation and systems.

2.3.3.1. INFOCON levels are prefaced with the term INFOCON, followed by ALPHA, BRAVO, CHARLIE and DELTA.

2.3.3.2. As the INFOCON threat escalates, specific network security requirements will be instituted that affect all aspects of network computing to include but not limited to:

2.3.3.2.1. Access to individual E-mail accounts.

2.3.3.2.2. Access to non-mission critical or mission essential systems, as defined by AFMAN 10-401*, Operation Plan and Concept Plan Development and Implementatio*n.

2.3.3.3. It is the responsibility of each group commander to provide the following information to the 939 ARW LAN Manager for inclusion to the 939 ARW LAN contingency and operating plan:

2.3.3.3.1. Identify the systems in use within their organization.

2.3.3.3.2. Provide the mission criticality definition of each system as defined in AFMAN 10-401.

2.3.3.4. The following actions are required by all personnel at all INFOCON levels:

2.3.3.4.1. Logoff the network when not in use.

2.3.3.4.2. Backup critical files to your hard drive.

2.3.3.4.3. Report any suspicious network or computer activity to your WM, 939 ARW LAN Manager or the command post (CP)

2.3.3.4.4. DO NOT open suspicious e-mail attachments.

2.3.3.4.5. DO NOT give out your network account information or password to anyone, especially if they state a need for it for network testing. ***HELPDESK OR NETWORK PERSONNEL WILL NEVER ASK YOU FOR THIS INFORMATION.***

2.3.3.4.6. Comply with any special guidance associated with the INFOCON status from your WM, 939 ARW LAN Manager or CP.

2.3.3.4.7. Be proactive and aware.

2.4. RECORDS MANAGEMENT. Users are responsible for ensuring received or transmitted information constitutes an Air Force record is maintained according to AFMAN 37-123, *Management of Records* and AFI 37-138, *Records Disposition Procedures and Disposition*. AFI 33-119, *Electronic Mail and E-Mail Management and Use*; **Paragraph. *8*** references E-mail, but should also be applied to other electronic transfer and storage such as use of file transfer protocol (FTP).

2.5. SUBSCRIPTION SERVICES. Subscription services may include professional newsgroups sponsored by Air Force and other federal, educational, and commercial agencies that may provide valuable information for users. Authorization is required by the user's commander, 939 ARW DAA, and 939 ARW CSO prior to use in accordance with AFI 33-119.

2.6. WEB SITE MANAGEMENT:

2.6.1. Placing Information on the intranet web pages:

2.6.1.1. Only information releasable to the general military or government and supports the wing mission will be placed on the wing Intranet web pages. No information will be posted on any publicly accessible web page except outside of the wing internet page. (See **Paragraph 2.6.2.**)

2.6.1.2. The following types of information **WILL NOT** be placed on the 939 ARW Intranet.

2.6.1.2.1. Classified information.

2.6.1.2.2. Privacy Act Information (AFI 33-332, *Air Force Privacy Act Program*).

2.6.1.2.3. For Official Use Only (FOUO) information and Freedom of Information Act (FOIA)-exempt.

2.6.1.2.4. Essential Elements of Friendly Information (EEFI) information.

2.6.1.2.5. Unclassified information that requires special handling, such as Encrypt for Transmission Only (EFTO), Limited Distribution, and Scientific and Technical Information. See AFI 61-204, *Disseminating Scientific and Technical Information*.

2.6.1.2.6. Product endorsements and commercial advertising, logos or trademarks.

2.6.1.2.7. Copyrighted or proprietary items unless permission is gained from the originator in writing.

2.6.1.3. Web Page Approval:

2.6.1.3.1. A letter of appointment designating the page provider will be provided to the web administrator prior to posting a web page on the 939 ARW Intranet site. This letter is not required if the WA provides and maintains the desired pages.

2.6.1.3.2. WA and WM personnel are the only individuals authorized to assign permissions to specific web pages.

2.6.1.3.3. The WA or WM will review requests for web page publication and have the responsibility to refuse publication of a web page in the event any published materials are deemed to be of a questionable nature (i.e. improper coordination, material may reflect adversely on the Air Force, security concerns, etc). 939 ARW LAN personnel also have the responsibility, should they identify existing web pages with significant problems (i.e. material may reflect adversely on the Air Force, sensitivity of material displayed, etc), to notify the page maintainer of the problem, and remove it immediately from the 939 ARW Intranet site.

2.6.1.4. Posting Web Pages:

2.6.1.4.1. The 939 ARW Intranet web pages will reside on the HQ AFRC controlled web server.

2.6.1.4.2. Failure to comply with the Air Force or lower level instructions concerning web pages is grounds for denial of service. In addition to Air Force guidance, web pages must meet the following criteria:

2.6.1.4.2.1. Each web page will include a link to the web provider and the information provider's e-mail.

2.6.1.4.2.2. The main 939 ARW Intranet web page will state all the required disclaimer notices, and every other page will have a link to the disclaimer page.

2.6.1.4.2.3. Web pages must be in good taste and may not contain any information, displays, etc, which may reflect adversely on the Air Force. They will not include any copyrighted material.

2.6.1.5. Any links to web pages outside the Intranet will be applicable to the wing and/or military mission. Links should be checked for currency and removed or relinked if required.

2.6.1.6. Web pages must be kept current and accurate. The information provider and page maintainer of a web page are responsible for the currency of web pages; any web pages that are not maintained properly should be removed.

2.6.1.7. OPSEC should be considered before placing any information on the intranet.

2.6.2. Placing Information On The Wing Internet Pages:

2.6.2.1. Commander and functional directors will:

2.6.2.1.1. Approve information both restricted and public placed on the web by their organization.

Ensure

2.6.2.1.2. Ensure all web pages are in compliance with DOD Policy and AFI 33-129.

2.6.2.1.3. Ensure content is mission-related, current and accurate.

2.6.2.1.4. Web pages may not contain privacy act, FOUO, or classified information.

2.6.2.2. Units will:

2.6.2.2.1. Continue to use the existing automated PA review and approval process for publicly accessible web pages.

Chapter 3

USE OF 939 ARW LAN AND ASSOCIATED SYSTEMS

3.1. GENERAL USE. Any activity on or through the 939 ARW LAN constitutes use of a government resource. Government-provided hardware and software are for conducting official and authorized government business. This does not prohibit commanders from authorizing personnel to use government resources if they determine it is in the best interest of the government and authorization is documented by letter, local operating instruction, or explicit policy. Using the 939 ARW LAN for other than authorized purposes may result in adverse administrative or disciplinary action.

3.2. OFFICIAL USE. There are no restrictions on official uses. Official uses include emergency communications that the Air Force determines are necessary in the interest of the federal government. Official use may include, when approved by theater commanders in the interest of morale and welfare, communications by military members and other DoD employees who are deployed for extended periods away from home on official DoD business.

3.3. AUTHORIZED USE.

3.3.1. As covered within AFI 33-119, and AFI 33-129.

3.3.2. Authorized personal use includes brief communications made by authorized users while traveling on US government business to notify family members of official transportation or schedule changes. It includes personal communications from the authorized user's workplace that are most reasonably made while at the workplace (such as checking in with spouse or minor children; scheduling doctor, automobile, or home repair appointments; brief Internet searches; or e-mailing directions to visiting relatives), when the unit commanders permits such categories of communications.

3.4. UNAUTHORIZED USE.

3.4.1. As covered within AFI 33-112 and AFI 33-114, *Software Managemen*t.

3.4.2. Additionally the following activities involving the use of government-provided computer hardware or software are specifically prohibited:

3.4.2.1. Installing any software, whether received in an official government capacity, purchased in addition to the standard software applications authorized, or personally owned without going through your WM for assistance or direction.

3.4.2.2. Changing AF, AFRC or locally implemented configuration settings, including but not limited to display settings.

3.4.2.3. Using personally owned equipment without going through your WM for assistance or direction.

3.4.2.4. Using personally owned personal digital assistants (PDA), such as Palms, Visors, IPAQs, or Jornadas are not authorized even with local permission.

3.4.2.5. Downloading freeware, shareware, personal internet provider, instant messaging, and telnet chat applications.

3.4.2.6. Sharing hard drives, removable drives and folders over the network.

3.4.2.7. Saving personal data to network shared drives.

3.4.2.8. Accessing unauthorized web sites from your government system.

3.4.2.9. Using unauthorized E-mail service. This includes but is not limited to all web based mail such as Hotmail.

3.4.2.10. Installing third party software for viewing of personal or civilian job related E-mail including but not limited to instant messaging.

3.4.2.11. Installing third party or peer to peer software for continuous web updates and free downloading services including but not limited to PointCast or any media related download sites.

3.4.2.12. Auto forwarding of your government E-mail to your personal or civilian job e-mail. Government e-mail must be protected from residing on commercial servers in order to protect privacy act material (PA), for official use only (FOUO), and possible classified information mistakenly delivered to an unclassified account.

3.5. USE OF PERSONAL HARDWARE AND SOFTWARE ON 939 ARW LAN. Use of personal hardware and software on 939 ARW LAN or systems connected to 939 ARW LAN must be identified in the systems accreditation package and approved by 939 ARW ECO, 939 ARW CSO and 939 ARW DAA. Exceptions are addressed above in paragraph **3.4.2.3.** Such use must be in accordance with AFI 33-202, *Computer Security*.

3.6. PREVENTING, MONITORING AND REPORTING ABUSE.

3.6.1. Preventing Abuse. Network/system managers will employ practical, cost effective methods to prevent users from accessing or transferring information that could reflect adversely on the Air Force or DoD or create an undue burden on the communications-computer system or result in significant cost to the government. This should include, but is not limited to, user education and blocking undesirable Internet sites (e.g., pornographic sites, hate literature sites). This may be extended to preventing access to sites that serve no benefit to the Air Force, primarily if the communication-computer system is becoming overburdened or the activity is impeding the conduct of official business or resulting in a significant cost to the government. Actions taken to prevent abuse should not interfere with beneficial uses of sites or services.

3.6.2. Monitoring Systems. If, in the course of day-to-day operations, suspicion of abuse or misuse of government systems arises, the suspicious activities must be reported according to the following paragraphs:

3.6.2.1. 939 ARW LAN personnel must report incidents according to AFSSI 5021, *Vulnerability and Incident Reporting.*

3.6.2.2. Any suspicious activity must be reported to the 939 ARW CSO.

3.6.2.3. The CSO will contact appropriate officials if waste, abuse, inappropriate or illegal activity is validated.

3.6.3. Reporting and Acting on Suspected Abuse. Abuse of government systems falls into two categories of illegal use: criminal use and general unauthorized use. Care must be taken when fixing blame for suspected abuse/activities. The identification of a PC or user account involved in suspicious

activity does not necessarily identify the actual offender. Legal advice/coordination must be obtained prior to taking action.

3.6.3.1. Illegal (Criminal) Use. If monitoring of government systems or reports of their use results in suspicion of illegal activity, the CSO will notify the Air Force Office of Special Investigations (OSI), 142 SFS/SPAI and 939 ARW/JA immediately.

3.6.3.2. General Unauthorized Use. If monitoring of government systems or reports of their use results in the suspicion of unauthorized use, the 939 ARW CSO must be notified. The nature/ severity of the unauthorized use will determine the corrective action to be taken. Activities which result in suspicion of significant violations (i.e., activities involving pornography, sexually explicit material, classified information at a level above that which is authorized on the system as covered within AF 33 series instructions) of a government system, must be acted upon. A sample letter will be provided to a commander upon initial investigation of the suspected abuse.

3.6.3.3. Based on initial fact- findings of the reported suspected violation, the CSO must report any significant findings to the group commander, residing over the equipment or personnel. The CSO will also provide a courtesy copy to the 939 ARW DAA, JA, SA, MSG/CC, and CF/CC.

3.6.3.4. Upon receipt of the CSO report, the commander will review and take action as deemed appropriate. The commander or appointed investigating officer may respond to the CSO in writing to request additional fact finding information or to request the cleansing of the computer system once the information is no longer needed for possible administrative action.

3.6.3.5. When the CSO receives the above request from the commander or investigating officer, the 939 ARW/JA will be contacted for concurrence. With this concurrence, the system is cleansed (all inappropriate electronic information is removed). It will then be returned to the work center.

3.6.3.6. In the event that additional reports are received for the same computer system, the fact finding process will remain the same. Upon three (3) violations, the computer system will be removed from the work center for a period of time to be determined by the severity of the abuse, through the CSO, JA and group commander with a report forwarded to the DAA. The entire work center must receive additional information assurance awareness training and education on the use and operation of government computer equipment and network capabilities.

3.7. ACCOUNTS.

3.7.1. All 939 ARW LAN users must complete IA Awareness Training prior to being granted access to the 939 ARW LAN IAW AFI 33-204, *Information Assurance (IA) Awareness Program.*

3.7.2. All individuals accessing the 939 ARW LAN must meet the investigative requirements of AFI 31-501, *Personnel Security Management Program,* Para 3.27.

3.7.3. All 939 ARW LAN account requests must be submitted using PIA Form 33-115, *Request for Network and System Access.*

3.7.4. Inactive 939 ARW LAN Accounts:

3.7.4.1. In order to assure information is safeguarded and the network is secure for all users, network accounts with no activity for more than 120 days are considered inactive.

3.7.4.2. Inactive accounts cause unnecessary overhead and increase network vulnerabilities since those accounts are not regularly monitored for suspicious activity.

3.7.4.3. All inactive accounts will be reviewed monthly by the LAN manager.

3.7.4.4. The 939 ARW LAN Manager will provide the CSO with an inactive accounts report.

3.7.4.5. The CSO will review and send a letter to each group commander with a listing of individuals with inactive accounts.

3.7.4.6. The inactive accounts will be closed and all associated files deleted 30 days following distribution of the letter unless the unit contacts the CSO to request an extension due to extenuating circumstances.

3.8. FILE MANAGEMENT.

3.8.1. The information usage and management apply to all 939 ARW personnel at Portland IAP, OR. It is the responsibility of 939 CF/SCBN network control center (NCC), System Administrators (SAs) workgroup managers (WMs), records managers and each commander to ensure adequate accounting and control procedures are in effect to properly manage this program.

3.8.2. To manage effectively our electronic information resources the following applies:

3.8.2.1. All domain administrators will ensure that application and system files are saved to the common applications (Apps) shared drive.

3.8.2.2. Data saved on the "Public" shared drive (P: drive) will only pertain to wing level.

3.8.2.3. Any information saved to the organizational drive (Y: drive) will be into an approved electronic file plan. All such information will be maintained in accordance with applicable records management disposition instructions.

3.8.2.4. The only files allowed on a user's home directory (Q: drive) are their personal address book and e-mail personal folders.

3.8.2.5. With exception to electronic data in **Paragraph 3.8.2.1.1**., there will be no archival of personal information on the PDXAFRES domain servers.

3.8.3. Privacy Act and for official use only (FOUO) data will be restricted access through user group or password protection. Enlisted Performance Reports (EPRs) and/or Officer Performance Reports (OPRs) are <u>not</u> allowed on the PDXAFRES domain servers.

3.8.4. Any electronic information found contrary to the above statement is subject to removal.

Chapter 4

INFORMATION PROTECTION AND SECURITY

NOTE: 939 ARW LAN POCs and 939 ARW LAN users must be aware of and adhere to virus procedures contained in this directive. Failure to adhere to the following guidance is grounds for denial-of-service by 939 ARW LAN personnel.

4.1. REPORTING PROCEDURES (ATTACKS, VULNERABILITIES, INCIDENTS, VIRUS, ETC). Report all automated information system (AIS) vulnerabilities, suspected intruder activity, security incidents, and virus (malicious logic) attacks to your SA, WM or the 939 ARW CSO. All reporting must be accomplished according to instructions outlined in AFSSI 5021. This does not negate other trouble, discrepancy, or incident reporting mandated by other directives (i.e., AFI 31-401, *Information Security Progra*m). Other 939 ARW LAN unique reporting requirements are incorporated into this instruction. All virus incidents must be reported according to AFSSM 5023, *Viruses and Other Forms of Malicious Logi*c, and AFSSI 5021.

4.2. ANTI-VIRUS SOFTWARE.

4.2.1. Use anti-virus software available through the 939 ARW LAN. The 939 ARW LAN will provide automatic updates to users through the local Norton Anti-Virus Corporate server. It is not authorized for any 939 ARW LAN user to go outside the network (such as the internet or through FTP channels) to download auto update capabilities through the anti- virus software sites. This is only accomplished by the LAN manager and is provided for all users on the 939 ARW LAN.

4.2.2. Systems Connected to 939 ARW LAN. All systems connected, directly or indirectly, to 939 ARW LAN will use antivirus software when such software is available for the system. Users may not disable anti- virus software. If an antivirus software package is creating problems on a system, request assistance from your WM, SCBN or CSO. If the CSO is unable to resolve the problem, the software package may be disabled; AFRC Network Operations Systems Center (NOSC) will be contacted to correct the problem. If AFRC is unable to resolve the problem, other DoD antivirus software must be utilized and documented for accreditation purposes.

4.2.3. All stand-alone systems (not connected to the 939 ARW LAN), such as notebooks/laptops or desktops not connected to the 939 ARW LAN, must obtain the available software and virus updates from the WM or the 939 ARW LAN Manager office weekly. A checklist shall be used to document compliance.

4.2.4. Where feasible, scan all incoming traffic for viruses before use.

4.2.4.1. The antivirus server will be configured to force client stations to perform automatic virus scans on a daily basis.

4.2.4.2. Virus scan any data media transported between computers at home and work (etc., floppy disks or CD-RWs.)

4.2.4.3. Virus scan all commercial off the shelf (COTS) software prior to installation on operational AIS.

4.2.5. 939 ARW LAN POCs include virus prevention, detection, eradication, and reporting procedures in user awareness training.

4.2.6. 939 ARW CSO will include awareness training through e-mail to all air reserve technicians (ART) and wing DoD civilian employees highlighting information to be passed on to all users.

4.3. VIRUS ERADICATION ASSISTANCE. Users requiring assistance with virus or suspected virus activity must first contact their WM, 939 ARW LAN Manager or the CSO.

4.4. REPEATED VIRUS INFECTION. Users and systems found to be repeatedly infected with a virus may be denied service by 939 ARW LAN personnel until their systems, disks, and practices are shown to be clean and unlikely to cause re-infection.

4.5. PASSWORD MANAGEMENT AND TERMINAL SECURITY.

4.5.1. Each user is responsible for meeting the basic criteria for password composition, length, life-cycle, ownership, distribution, entry, authentication period, and safeguarding, as set forth in applicable AF directives. The following provides password and terminal rules and guidance for users of 939 ARW LAN.

4.5.1.1. 939 ARW LAN Access. Initial passwords to access 939 ARW LAN will be issued after completion of the training in accordance with paragraph **3.7.** 939 ARW LAN personnel do not create or provide default passwords and do not provide them over the phone. Each user will contact the appropriate WM or 939 ARW LAN Manager office and present the proper identification to obtain an account and set his/her password

4.5.1.2. Unattended PCs/Terminals/Workstations. If a terminal needs to be left unattended while logged in to 939 ARW LAN, a screen saver must be used with the password option activated or use the ctrl+alt+delete function to lock the workstation.

4.5.1.3. As a minimum, all unattended workstations will be password protected. Those users who do not comply with this policy will have their computers set with a password enabled screen saver with a default timeout of 5 minutes.

4.5.2. Other Password Rules/Guidance:

4.5.2.1. At a minimum, you must safeguard all passwords as “For Official Use Only” (FOUO).

4.5.2.2. Do not set 939 ARW LAN or leave e-mail passwords set to ‘password.’

4.5.2.3. 939 ARW LAN account and e- mail passwords must use a mixture and at least one of each of the four following choices; upper case, lower case, numeric, and special characters (~!@#$%^*()+).

4.5.2.4. Passwords must be at least eight characters in length.

4.5.2.5. Password cannot be one of the last five passwords used.

4.5.2.6. Enter passwords in such a manner that the password is not revealed to anyone observing the entry process.

4.5.2.7. Protect your password so you are the only one to know it. No one from 939 ARW LAN will ask for your password in person or over the phone. Do not let other individuals use your account.

4.5.2.8. Contact your WM or 939 ARW LAN Manager if you suspect your password has been compromised.

4.5.2.9. Passwords Sample: %Iwnt$$2dY

4.5.2.10. Do not construct passwords related to:

4.5.2.10.1. Your personal identity or other identifiers such as SSN, phone numbers or a license plate number or family.

4.5.2.10.2. Passwords from the dictionary, slang words, names, or profanity.

4.5.2.10.3. Placing a single number at the beginning or ending of a password does not prevent it from being cracked. Most password cracking programs will check for and crack these passwords.

4.5.2.11. Please be aware the CSO continuously runs automated vulnerability software which checks for ineffective passwords. Any user whose password does not meet Air Force criteria will have their account disabled and be directed to change their password.

Chapter 5

ADDING AND MAINTAINING 939 ARW LAN CONNECTIONS

5.1. ADDING 939 ARW LAN CONNECTIONS.

5.1.1. All connections to 939 ARW LAN must be authorized by the 939 ARW LAN Manager, CSO and DAA. All connections must adhere to 939 ARW Certification and Accreditation (C&A) in conjunction with the 939 ARW System Security Authorization Agreement (SSAA). To add new users to the 939 ARW LAN, please refer to **Chapter 3**, paragraph **3.7.**. Exceptions to the C&A and SSAA must be documented via letter of agreement/memorandum of agreement (LOA/MOA) and indorsed by the CSO and DAA. All changes to an existing 939 ARW LAN connection must be authorized by the 939 ARW LAN Manager and CSO. Changes include, but are not limited to:

5.1.1.1. Adding hubs, ports, routers, etc. to existing connections.

5.1.1.2. Changing a user LAN connection or a network printer connection.

5.1.1.3. Changes regarding modems including modem configuration changes, etc.

5.1.2. All requests for connections, changes, or services require an approved AF Form 3215, *C4 Systems Requirements Document*, be submitted to 939 CF/SCBN office.

5.1.3. Each AF Form 3215 will be reviewed, approved or disapproved for security, feasibility, standards as set by AF, HQ AFRC, host base and the 939 ARW C2WG standards.

5.2. ACCREDITATION/APPROVAL TO OPERATE.

5.2.1. IAW AFI 33-202, *Computer Security,* all systems connected to 939 ARW LAN must have a current, up-to-date, approval to operate (accreditation) signed by the DAA. For assistance, contact your SA, WM, 939 ARW LAN Manager or CSO. Certain desktop systems fall under the 939 ARW LAN accreditation umbrella and do not require a separate accreditation. The list below describes non standard systems. If any desktop system meets any of the following criteria it must have separate approval to operate on the 939 ARW LAN:

5.2.1.1. Software not standard to a 939 ARW LAN desktop. Reference **Paragraph 6.3.** below.

5.2.1.2. A modem connected to a phone line.

5.2.1.3. A connection to a non-939 ARW LAN system, even if the connection is not active during 939 ARW LAN sessions.

5.2.1.4. Operates in a classified mode.

5.2.1.5. Intended for use in a stand-alone (separate from 939 ARW LAN) mode.

5.2.1.6. Any feature (software, hardware, connection, etc) making the system significantly different from a standard 939 ARW LAN desktop machine.

5.3. ACCREDITATION REVIEW. Copies of signed approval to operate letters, as required above, must be forwarded to the 939 ARW CSO, along with the accreditation package for review.

5.4. MODEMS.

5.4.1. Modems pose a significant risk to the 939 ARW LAN. Improperly connected/configured modems can allow access to the 939 ARW LAN by unauthorized personnel, circumventing security barriers to prevent such access. All PCs with modems connected to phone lines must be identified in the PCs accreditation package and to the 939 ARW LAN CSO. Justification for the modem connection and configuration information must be included in the accreditation package. Configuration information must include, but is not limited to, status of dial- in capabilities. 939 ARW LAN users must submit an AF Form 3215 for any of the following:

5.4.1.1. Plugging a modem in to a phone line.

5.4.1.2. Changing configuration settings on a modem.

5.4.1.3. The AF Form 3215 must be reviewed by the 939 ARW LAN Manager and CSO.

5.4.1.4. Once approved by the 939 ARW LAN Manager and the CSO, the change must be updated in the 939 ARW LAN accreditation package and the PCs accreditation package.

5.4.1.5. Any modem connection allowing dial- in capability to the PC on 939 ARW LAN must be approved by the CSO and DAA prior to activation of dial-in capability.

Chapter 6

SOFTWARE MANAGEMENT PROGRAM

NOTE: The 939 ARW software management policies, as outlined in the paragraphs below, apply to all 939th Air Refueling Wing personnel at Portland IAP, OR. It is the responsibility of 939 CF/SCBN network control center (NCC), each commander, and the workgroup managers (WMs) to ensure adequate accounting and control procedures are in effect to properly manage this program.

6.1. 939 ARW SOFTWARE MANAGEMENT.

6.1.1. WMs will originate all new software purchases using an AF Form 3215 for justification. Information Assurance (IA) and NCC coordination are required prior to purchase and/or use.

6.1.2. IA must keep all original software and licenses in a secure cabinet. IA will maintain a written inventory of original software, licenses, and keys which will be kept up to date at all times. This inventory must match the systems management server (SMS) and Bell Manage application inventory maintained by the network configuration manager.

6.1.3. The NCC will receive and inventory network software, test and validate new software applications and network operating systems.

6.1.4. New software included with a new computer system must be inventoried by WMs and added to the software management database maintained by IA.

6.1.5. Virus checks will be ongoing using server-managed Norton Anti-virus. Norton Anti-virus will be activated at all times.

6.1.6. To maintain software releases and updates, the NCC and WMs will use a combination of SMS automated updates and suspense implementation.

6.1.7. Removal of unauthorized software.

6.1.7.1. It is the users responsibility to justify the use of the software using the software authorization process as outlined in **Paragraph 6.1.2.**

6.1.7.2. If unauthorized software is found, it will be removed immediately.

6.1.8. 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 wing communications and information systems officer (CSO) has authorized such use. When authorized for installation on a home computer, the software may be used only for official AF business. Do not make any copies of copyrighted software.

6.1.9. WMs and the network configuration manager will conduct a software inventory and IA will review site license agreements once a year. Recommend the month of February following annual IPMS systems inventory.

6.2. SOFTWARE LICENSING. Care must be taken to ensure compliance with software licensing/copyright agreements. All 939 ARW LAN POCs and WMs must be familiar with software licensing rules. These individuals are responsible to ensure 939 ARW LAN users in their unit or area, are familiar with licensing rules. Failure to adhere to licensing agreements is grounds for legal and or disciplinary administrative action, in addition to denial of service by 939 ARW LAN personnel.

6.3. SERVED NETWORK SOFTWARE. Served network software is software residing on a network server, intended to be run by users on their desktop PC. This software may not be copied to the local desktop PC disk drive(s), floppies, or other network drives by users. Doing so, may violate software licensing agreements. If any served software is installed separately on a desktop PC hard drive, the user (unit) must be able to produce documentation proving a software license exists that is dedicated to that PC or a site license that covers that PC.

6.4. CHANGING SOFTWARE ENVIRONMENT. Due to the continuously evolving 939 ARW LAN environment, the CSO is responsible to periodically update a list of 939 ARW LAN software. This list will indicate 939 ARW LAN software packages authorized on the local PC and those only authorized to be served out from a network server (not authorized on the local PC without an independent license). This listing will be made available to users upon request and through the 939 ARW Intranet Site, Support Group/Communications Flight web site.

6.5. CONTINGENCY BACKUP OFFICE AUTOMATION SOFTWARE. Units desiring to maintain software on the local PC in the event of a 939 ARW LAN outage, or for any other reason, must have independent software licenses dedicated to that PC (or appropriate site license).

6.6. COPYRIGHTED SOFTWARE INTRODUCED TO 939 ARW LAN SERVERS. Users are not authorized to copy, install, download, or backup copyrighted software or executable software (e.g., '.exe' files) to 939 ARW LAN servers (e.g., 'Y', 'W' or unit designated drives, etc). Exceptions must be approved by the 939 ARW LAN Manager and CSO via an AF Form 3215. Additional space required by a user must also be submitted on an AF Form 3215 to the user's WM.

6.7. ENSURING COMPLIANCE. All units/agencies with desktop PCs connected to 939 ARW LAN are subject to 939 ARW LAN software licensing compliance reviews by the CSO, 939 ARW LAN personnel, or WM within your group. Lack of cooperation (i.e., access to PCs connected to 939 ARW LAN) during such reviews or inability to produce requested licensing documentation for PCs connected to 939 ARW LAN are grounds for denial-of-service by 939 ARW LAN personnel. All 939 ARW units will conduct inventories of software and licenses at least annually. Software copyright violations must be resolved via removing software in question or taking appropriate action (i.e., purchasing software, and locating licenses).

Chapter 7

CLASSIFIED PROCESSING

7.1. CLASSIFICATION. 939 ARW LAN is a sensitive but unclassified AIS. Processing classified information on 939 ARW LAN is prohibited. Processing includes, but is not limited to, viewing, printing, creating, transferring, editing, downloading, uploading, opening, copying, and transmission of classified information over 939 ARW LAN.

7.2. SECURITY INCIDENTS. When classified information has been identified as having been introduced to 939 ARW LAN (i.e., e-mail, user or group network drive, PC connected to 939 ARW LAN, etc.) or any other unclassified systems or equipment, the following requirements must be followed. (Contamination occurs via ANY activity involving classified information on an unclassified system):

7.2.1. Incidents involving information that is suspected to be classified will have the classification verified by the appropriate OPR and/or via the security classification guide prior to initiating the sanitizing process.

7.2.2. The 939 ARW LAN Manager or CSO will initiate a lockdown of the affected account, file or system, in order to protect the potentially classified information until a final determination has been made.

7.2.3. Simply deleting E-mail or disk files ***IS NOT*** sufficient to clean up classified information on an automated system, no matter how minor you feel the incident or type activity is. Just viewing or printing a classified document can contaminate a system, requiring clean up, even if you didn't save it.

7.2.4. DO NOT delete or destroy anything (E-mail, disk files, hard copies, etc). The 939 ARW LAN Manager and CSO must have specific information about the suspected documents or information in order to ensure thorough clean up is accomplished. This is required to verify the clean-up process was successful. If adequate information is not available, security team personnel may require affected equipment's hard drives be completely wiped vice 'surgical wiping'.

7.2.5. Immediately notify the 939 ARW LAN Manager or CSO (or HQ AFRC/NOSC if after normal duty hours). Specific information about the location of classified information that has been introduced to an unsecured system is, at a minimum, extremely sensitive information (i.e., user name, user ID, PC location, etc), especially when identifying the fact that there may be classified information contained thereon. If the 939 ARW LAN Manager or CSO cannot be notified in a reasonable amount of time, the following must be accomplished:

7.2.5.1. Discontinue use of contaminated systems and physically disconnect the contaminated system from all unclassified connections until the system has been sanitized or sanitation procedures require reconnection.

7.2.5.2. Change all involved passwords and handle as classified at the level of classified information involved. For e-mail incidents be sure to password access all contaminated E-mail folders as well as your main 939 ARW LAN logon password. (Exchange uses the 939 ARW LAN logon password to access your E-mail on the Exchange server.) Notify your ISSO or equivalent. (The ISSO may be identified as the WM).

7.2.5.3. Provide assistance to and follow any procedures provided by 939 ARW LAN personnel. Failure to follow instructions provided by 939 ARW LAN personnel may result in denial of ser-

vice and could result in administrative or disciplinary action for failure to protect national security information.

7.2.5.4. Secure all classified materials in approved containers. Secure contaminated equipment based on the level of classified involved and the degree of security provided by your facility, the duration over which the equipment will remain contaminated, and the magnitude of the incident (i.e., number of users involved). If the incident involves a contaminated PC, change or activate the PC BIOS password via the PCs setup process.

7.2.5.5. Notify your wing security manager. Handle and report the incident as an information security incident according to AFI 31-401.

7.2.6. 939 ARW LAN Manager or CSO will:

7.2.6.1. Take all necessary actions to ensure protection and sanitation of affected network systems using methods fulfilling the requirements of AFSSI 5020, *Magnetic Remanenc*e. Reasonable efforts must be made, first, to protect the classified information, and second, to sanitize all affected accounts and systems as expeditiously as possible. Deviation from standard sanitation methods due to extenuating circumstances (i.e., mass contamination of user accounts/PCs, etc) must be coordinated through 939 ARW DAA, HQ AFRC/NOSC and the owner/originator of the classified information.

7.2.6.2. Protection Via 939 ARW LAN Shutdown or Isolation (partial or complete). Contemplating shutdown or isolation of 939 ARW LAN must take into account the following:

7.2.6.2.1. Level of classified involved and its potential damage to national security if compromised or further compromised. Consult appropriate agencies when special category information is involved.

7.2.6.2.2. How widespread the contamination is.

7.2.6.2.3. Amount of time it will take to disable affected accounts.

7.2.6.2.4. Amount of time it will take to sanitize accounts and systems involved.

7.2.6.2.5. General exposure/vulnerability of the information to compromise.

7.2.6.2.6. Cost in work hours due to unavailability of network resources to users and organizations.

7.2.6.3. Disable (make inaccessible) affected user accounts and e- mail accounts until contaminated accounts are sanitized or until access is required for the sanitation process.

7.2.6.4. Provide users and ISSOs instructions and assistance.

7.2.6.5. Request assistance from the HQ AFRC/NOSC as needed.

7.2.6.6. Report the incident to the 939 MSS/SFI, HQ AFRC/NOSC, and HQ NAF.

7.2.6.7. Provide the necessary information and cooperation to ensure all contaminated systems outside 939 ARW LAN are notified of the incident and provide necessary information to aid in sanitizing their systems.

Chapter 8

MANAGING COMMUNICATIONS AND COMPUTER EQUIPMENT AND SOFTWARE

8.1. ACCOUNTABILITY. All 939 ARW communications and computer equipment and software are accountable government assets. Government assets are managed by a strict set of rules to protect government resources from misuse, theft, damage, or destruction. The CSO will determine the items to be included in the accountability system, Information Protection Management System (IPMS).

8.1.1. AFI 33-112 states that any item of $500 or more must be tracked within IPMS. For 939 ARW, equipment or software that may be considered of significant value and pilferable will be tracked regardless of the cost of the equipment or software. Higher headquarters, wing DAA and 939 ARW LAN Manager will establish policy and guidance on what is of significant value and pilferable.

8.1.2. All software whether freeware, shareware or licensed is accountable.

8.2. RESPONSIBILITIES. Responsibilities on the management of communications and computer (C4) equipment and software are outlined in AFI 33-112 and AFI 33-114. This instruction supplements higher headquarters direction.

8.3. ACQUISITION MANAGEMENT REQUIREMENTS.

8.3.1. Centrally Purchased.

8.3.1.1. What is required to be purchased through the IT IPMAC card, tracked through IPMS, or monitored for support:

8.3.1.1.1. All computer hardware and associated equipment.

8.3.1.1.2. Computers (desktop/laptop), monitors, internal/external hardware (ram, hard drives, video, sound, all internal expansion cards).

8.3.1.1.3. Scanners, digital cameras, portable projectors, printers, facsimile, copiers.

8.3.1.1.4. Personal digital or handheld PCs (i.e. Palm, IPAQ, etc.) and all accessories.

8.3.1.2. Anything that is questionable should be directed to your WM.

8.3.2. Individually Purchased.

8.3.2.1. What is not required to be purchased through the IT card, tracked through IPMS, or monitored for support:

8.3.2.1.1. Any computer consumables.

8.3.2.1.2. Diskettes, CD recordable discs, zip disks, jaz cartridges, printer toner, inkjet cartridges, or paper.

8.3.2.1.3. Mouse/mice, keyboards/external drives, external/internal battery supplies, cables, and uninterruptible power supplies (UPS).

8.3.2.2. Report problems with printer toner cartridges obtained through the mandatory source with the following information:

8.3.2.2.1. Documented explanation of the problem for each occurrence.

8.3.2.2.2. Documented repair costs if necessary.

8.3.2.2.3. Forward to 939 CF/SCB, FM and the supplier. This documentation will provide background material for any waivers that may be considered in the future.

8.4. INFORMATION TECHNOLOGY (IT) GOVERNMENT ACQUISITION PROCEDURES.

8.4.1. Each user will request items stated in **Paragraph 8.3.** using an AF Form 3215, routed through their WM.

8.4.2. Each WM provides the initial technical solution with cost associated and concur/nonconcurring statement. If nonconcurring, the WM provides alternative work-arounds, may request additional information or may recommend disapproval providing sufficient justification.

8.4.3. Each WM ensures the AF Form 3215 is routed through the appropriate supervisor, resource advisor, and group commander (as required).

8.4.4. Upon completion of all required staffing of the AF Form 3215, the WM forwards it to the 939 ARW LAN Manager.

8.4.5. The LAN manager assigns the AF Form 3215 tracking number, reviews the technical solution provided and updates the costs associated with the purchase and forwards to the CSO.

8.4.6. If the request is for software, the wing CSO must sign the AF Form 3215.

8.4.7. 939 ARW LAN Manager sends an E-mail to the unit RA, CR, RA,WM and FM to transfer funds. This E-mail notification is your approval document to be maintained with your O&M funding records.

8.4.8. The appropriate RA returns e-mail to LAN manager, CFs RA, and FM, with a courtesy copy to the WM.

8.4.9. If the item is to be purchased via wing IT card the CFs RA will cut an AF Form 4009, *Government Purchase Card Fund Cite Authorization* for monies to be transferred to the IT card. FM transfers the funds as requested and if available.

8.4.10. FM returns e-mail to the CFs RS and courtesy copies SCBN, the RA and WM.

8.4.11. 939 ARW LAN Manager orders the item requested on the AF Form 3215 and provides an E-mail notification to the WM and RA and FM of the date, amount of purchase and an approximate date to receive the item.

8.4.12. Upon receipt, 939 ARW LAN Manager will maintain all purchasing documentation.

8.4.13. If required, the equipment or software is entered into IPMS, labeled accordingly and the WM is notified to pick up the item.

8.5. REPORTS OF SURVEY.

8.5.1. The 939 ARW LAN Manager will ensure the guidance and procedures for conducting reports of survey (ROS) investigations established by the host base ROS program managers and AFMAN23-220, *Reports of Survey for AF Property,* is followed if IT property is lost, damaged or destroyed.

8.6. PRESCRIBED FORMS. This instruction directs the use of PIA Form 33-115, *Request for Network and System Access.*

MARK A. KYLE, Col, USAFR
Commander, 939 ARW

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

AFI 31-401, *Managing the Information Security Program*

AFPD 33-1, *Command, Control, Communications, and Computer (C4) Systems*

AFPD 33-2, *C4 Systems Security*

AFI 33-112, *Computer Systems Management*

AFI 33-114, *Software Management*

AFI 33-119, *Electronic Mail (E-Mail) Management and Use*

AFI 33-129, *Transmission of Information Via the Internet*

AFI 33-202, Computer Security

AFI 33-204, *Information Assurance (IA) Awareness Program*

AFI 33-219, *Telecommunications Monitoring and Assessment Program (TMAP)*

AFMAN 37-123, *Management of Records*

AFMAN 37-132, *Air Force Privacy Act Program*

AFI 37-138, *Records Disposition Procedures and Disposition*

AFI 61-204, *Disseminating Scientific and Technical Information*

AFMAN 10-401, Vol 1, *Operation Plan and Concept Plan Development and Implementation*

AFMAN 23-220, *Reports of Survey for Air Force Property*

AFSSI 5020 (future AFMAN 33-224), *Remanence Security*

AFSSI 5021 (future AFMAN 33-225), *Vulnerability and Incident Reportin*g.

AFSSM 5023, *Viruses and Other Forms of Malicious Logic*

DoDR5400.7/AF Sup, *DoD Freedom of Information Act Program*

AF Form 3215, *Communication and Computer System Requirements Document*

AF Form 4009*, Government Purchase Card Fund Cite Authorization*

PIA Form 33-11*5, Request for Network and System Access*

Abbreviations and Acronyms

ADPEC—Automated Data Processing Equipment Custodian

AFNCC—Air Force Network Control Center

AFSSI—Air Force Systems Security Instruction

AFSSM—Air Force Systems Security Memorandum

AIS—Automated Information System

ASIMS—Automated Security Incident Measurement System

AO—Approving Official

C2WG—Communications and Computer Working Group

C4—Command, Control, Communications, and Computers

C&A—Certification and Accreditation

CCB—Configuration Control Board

CM—Configuration Management

COMPUSEC—Computer Security

COMSEC—Communications Security

COTS—Commercial Off-The-Shelf

CSM—Computer Systems Manager

CSO —Computer Security Officer or Communication and Information Systems Officer

DAA—Designated Approving Authority

DBMS—Database Management System

DISA—Defense Information Systems Agency

DoD—Department of Defense

EC—Equipment Custodian

ECO—Equipment Control Officer

EEFI—Essential Elements of Friendly Information

EMSEC—Emissions Security

FM—Finance

FOIA—Freedom of Information Act

FOUO—For Official Use Only

GPC—Government Purchase Card

GPCPA—Government Purchase Card Purchasing Agent

IA—Information Assurance

IAO—Information Assurance Officer

IO—Investigating Officer

IPMS—Information Protection Management System

ISSO—Information Systems Security Officer

IT—Information Technology

LAN—Local Area Network

NAR—Network Account Request (NAR)

NCC—Network Control Center

NOSC—Network Operation System Center

PA—Privacy Act

RA—Resource Advisor

ROS—Reports of Survey

SBU—Sensitive But Unclassified

SMSP—System Management and Security Policy

SSAA—System Security Authorization Agreement

TASO—Terminal Area Security Officer

TCM—Telephone Control Monitor

TMAP—Telecommunications Monitoring and Assessment Program

USER-ID—User Identification

WA—Web Administrator

WM—Workgroup Manager

WPM—Web Page Maintainer

Terms

939 ARW LAN—Air Force Reserve Rescue Wing on Portland IAP OR primary administrative local area network and associated systems (i.e. web servers, etc).

939 ARW LAN POC—Individual assigned the additional duty of CSSO, TASO, TCM, and WPM.

Accreditation—Written documentation by a designated approving authority (DAA) that a C4 system is approved to operate in a particular security mode using a prescribed set of security features or safeguards for a specified period of time.

Automated Information System—Any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data and includes software, firmware, and hardware. **NOTE:** The term "AIS" includes stand-alone systems, communications systems, and computer network systems of all sizes, whether digital, analog, or hybrid; associated peripheral devices and software; process control computers; security components; embedded computer systems; communications switching computers; personal computers; workstations; microcomputers; intelligent terminals; word processors; automated data processing (ADP) systems; office automation systems; application and operating system software; firmware; and other AIS technologies, as developed.

Certification—Comprehensive evaluation of the technical and non-technical security features, and countermeasures of an AIS to establish the extent to which a particular design and implementation meet a set of specified security requirements.

Certification and Accreditation—C&A is a method for ensuring that appropriate combinations of security measures are implemented to counter relevant threats and vulnerabilities.

Certifying Official—Individual responsible for making a technical judgment of the AIS compliance with stated security requirements and requesting approval to operate from the DAA.

Communications-Information Systems Officer or Computer Security Officer(CSO)—The term CSO identifies the supporting CSO at all levels. The commander of the communications flight is the primary CSO for the 939 ARW; the information assurance officer is the alternate CSO for the wing. At MAJCOM and other activities, it is the person designated by the commander as responsible for overall management of communications- information systems budgeted and funded by the MAJCOM or activity. The CSO function uses the office symbol "ARW/CSO" which is expanded to three and four digits to identify specific functional areas. CSOs are the accountable officers for all automated data processing equipment in their inventory.

Computer System(s) Manager (CSM)—Official with supervisory or management responsibility for an organization, activity, or functional area that owns or operates an AIS. The CSM is operationally and administratively responsible for a system's mission performance. The CSM establishes and monitors the security program for a system and approves procedures at its remote sites. The CSM is responsible for security for the system's facility. For office automation systems, the CSM is usually the office chief. **(Note:** they are normally the senior communications officer, office chief, etc.). The CSM obtains approval to operate from the DAA prior to operating their system(s). They plan and program budgetary, manpower, and training support for the operation and security of the system. They also develop administrative procedures (controls) to ensure the secure operation of the system.

Countermeasure—The sum of a safeguard and its associated controls.

Data Aggregation—The convergence of information. This becomes a problem when certain information or data elements at one sensitivity level, requires reclassification at a higher level when combined or associated with other information. Aggregate data would require classification if the new information meets the specific classifying criteria as defined in DoD 5200.1-R or reclassification according to classification guidance provided by the functional OPR.

Designated Approving Authority (DAA)—Official with the authority to formally assume responsibility for operating an AIS or network within a specified environment.

End Users—The end users support the certification process by providing statement-of-need, operational concepts, and security requirements inputs to the PM and certifying official.

Essential Elements of Friendly Information (EEFI)—Key questions likely to be asked by adversary elements about specific friendly intentions, capabilities, and activities, so as to obtain answers critical to their operational effectiveness. (Joint Pub 1-02*, Department of Defense Dictionary of Military and Associated Term*s) (Valid answers to EEFI normally constitute classified information)

Firewall—A protection scheme that assists in securing internal systems from external systems.

Functional Office of Primary Responsibility (OPR)—Organization (e.g., division, directorate, or unit) that employs, but may not own, an AIS to perform its mission (function). **NOTE:** Normally, they own the data that is stored or processed on the AIS.

Home Page—A starting point or center of an info structure on the WWW. A typical home page will consist of hypertext links (pointers) to other web documents.

Incident—Unauthorized access or entry (or attempt) to an AIS. It can include browsing; disruption or denial of service; alteration or destruction of input, processing, storage, or output of information; or changes to AIS hardware, firmware, or software characteristics with or without the user's knowledge, instruction, or intent.

Information Protection Office—Formerly C4 Systems Security Office (ISSO).

Information Systems Security Officer (ISSO)—Official who manages the COMPUSEC program for an AIS assigned to them by the CSM; including monitoring AIS activities, and ensuring that the AIS is operated, maintained, and disposed of according to security policies and practices. The ISSO administers the system security policy in the operational environment, performs security-related tasks as required by the DAA, and ensures that only the system maintainer modifies the system. The ISSO prepares certification and accreditation plans for systems as defined in Section D. The ISSO maintains certification for the fielded system. The ISSO assists in the development of the system security policy and ensures compliance on a day-to-day basis. They identify and/or report security incidents, provide user training, and identify pending system or environment changes that may require re-certification or re-accreditation of the system. The ISSO must be intimately involved during pre-certification, certification, and accreditation phases of the C&A process. Their most important role is during the post-accreditation phase where they ensure the security posture of the system and the accreditation are maintained.

Internet—An informal collection of government, military, commercial, and educational computer networks using the Transmission Control Protocol/Internet Protocol (TCP/IP) to transmit information. The global collection of interconnected local, mid-level, and wide area networks that use IP as the network layer protocol.

Intranet—A restricted-access network that works like the web, but isn't on it. Usually owned and managed by an organization, an intranet enables an activity to share its resources with its employees without sensitive information being made available to everyone with internet access. Intranets may allow connection outside of the intranet to the internet through firewall servers and other security devices that have the ability to screen messages in both directions so that the organizations security is maintained.

Intruder—Unauthorized person who accesses an AIS with or without an unlawful intent. Typically an intruder breaks into a system for the challenge of defeating the system's security features.

Local Area Network (LAN)—A telecommunications system, within a small, specified geographical area, designed to allow a number of independent devices to communicate with each other over a common transmission topology. LANs are usually restricted to relatively small geographical areas (i.e., rooms, buildings, or clusters of buildings) and utilize fairly high data rates. Depending on the implementation, these communications networks can provide internal interchange of voice, data, graphics, video, or other forms of electronic messaging.

Log in—Procedure used to establish the identity of the user, and the levels of authorization and access permitted.

Log off—Procedure used to end a user's access to a system.

Malicious Logic—Intentional inclusion of hardware, firmware, or software to disrupt AIS availability, integrity, or confidentiality. **NOTE:** Trojan Horse is a form of malicious logic.

Network Account—User ID & Password which allow a user to log on and access resources on the 939th Local Area Network.

Network Manager (NM)—The individual who is responsible for the operation of a network.

Page Maintainer—The creator and, or focal point for specific material posted on the organization's home page.

Password—Protected and private character string used to authenticate an identity or to authorize access to data.

Penetration—The successful unauthorized access to an AIS or act of bypassing the AIS security controls.

Personal Password—Password known by one person and used to authenticate that person's identity.

Risk Management—The total management process of identifying, measuring, controlling, and minimizing uncertain events affecting AIS. **NOTE:** Risk management activities directly support certification and affect the accreditation decision.

Safeguards—Protective measures and controls prescribed to meet the security requirements of AIS. **NOTE:** Safeguards include security features and management constraints from the various security disciplines (i.e., administrative, procedural, physical, personnel, communications, emanations, and computer security), used in concert to provide the requisite level-of protection.

Security Feature—A hardware, firmware, or software controlled access protection to meet the security requirements of identification and authentication (I&A), mandatory access control (MAC), discretionary access control (DAC), object reuse, or audit. Security features are a subset of AIS security safeguards.

Sensitive, But Unclassified (SBU) Information—Unclassified information that is considered sensitive because it requires protection due to the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the data. The term includes information whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary data, records about individuals requiring protection under the Privacy Act, and data not releasable under the Freedom of Information Act. (Office of Management and Budget Circular No. A-130, Dec. 12, 1985.) See **Attachment 2** of AFSSI 5102 for identifying SBU information.

Software—A set of computer programs, procedures, and associated documentation concerned with the operation of a data processing system, e.g., compilers, library routines, manuals, and circuit diagrams. (See JP 1-02.)

System Security Policy—Set of laws, rules, and practices that regulate how sensitive (SBU and classified) information is managed, protected, and distributed by an AIS. **NOTE:** System security policy interprets regulatory and operational requirements for a particular system and states how that system will satisfy those requirements. All systems or networks that process SBU or classified information, will have a security policy.

Threat—Current and perceived capability, intention, or attack directed to cause denial of service, corruption, compromise, or fraud, waste, and abuse to a system.

Unit COMPUSEC Manager—The unit COMPUSEC manager is the single individual within each organization responsible for developing and managing the COMPUSEC program on a day-to-day basis. Normally, they require assistance and assign ISSOs to particular systems or groups of systems.

User—Person or process accessing an AIS by direct connections (e.g., via terminals) or indirect connections.

User Representative—The user representative is the focal point for the end users. They provide the voice in identifying the user's roles, responsibilities, and capabilities. The user representative, at minimum, reviews and approves the security requirements, assurance factors, certification results, and any proposed security features.

User Identification (User-id)—Unique symbol or character string used by an AIS to uniquely identify a specific user.

Vulnerability—Defense weakness to control a threat to the AIS.

Web Document—A physical or logical piece of information on the WWW.

Web Page—A single document that includes the text of the document, its structure, any links to other documents, images, and other media.

Web Server—A software/hardware combination that provides information resources to the WWW.

Web Server Administrator—The system administrator for the web server, usually referred to as the "Webmaster."

World Wide Web (WWW)—Uses the internet as its transport media and is a collection of protocols and standards that allow the user to find information available on the internet by using hypertext and/or hypermedia documents.