

**BY ORDER OF THE
SECRETARY OF THE AIR FORCE**

AIR FORCE INSTRUCTION 33-114

1 JULY 2000



**910 AIRLIFT WING
Supplement 1**

1 OCTOBER 2001

Communications and Information

SOFTWARE MANAGEMENT

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: HQ AFCA/ITC (Mr. John H. Derrell)

Certified by: HQ USAF/SCXX
(Lt Col Terry G. Pricer, Sr.)

Supersedes AFI 33-114, 30 June 1994.

Pages: 24
Distribution: F

This Air Force instruction (AFI) implements Executive Order (E.O.) 13103, *Computer Software Piracy*, September 30, 1998; Department of Defense Directive (DoDD) 3405.1, *Computer Programming Language Policy*, April 2, 1987; and Air Force Policy Directive (AFPD) 33-1, *Command, Control, Communications, and Computer (C4) Systems*. It identifies responsibilities for management of commercial off-the-shelf (COTS) and Air Force-unique software acquired by the Air Force (other than software internal to a weapon system; see AFPD 63-1, *Acquisition System*). Send recommended changes or comments to Headquarters Air Force Communications Agency (HQ AFCA/ITPP), 203 W. Losey Street, Room 1065, Scott AFB IL 62225-5222, through appropriate channels, using AF Form 847, **Recommendation for Change of Publication**, with an information copy to HQ AFCA/ITC, 203 W. Losey Street, Room 3065, Scott AFB IL 62225-5222. Refer to **Attachment 1** for a glossary of references and supporting information.

(910AW) The OPR for this supplement is 910 AW/CF (Judy Hendricks). This supplement implements and extends the guidance of Air Force Instruction (AFI) 33-114, 1 July 2000. The AFI is published word-for-word without editorial review. 910 AW supplementary material is indicated by (910 AW) in bold face type. This supplement describes 910 AW procedures to be used in conjunction with the basic instruction. Upon receipt of this integrated supplement discard the standalone Air Force basic. It applies to all base personnel and tenants.

SUMMARY OF REVISIONS

This document is substantially revised and must be completely reviewed.

This revision removes all acquisition-related material and functions. It includes policy and management structure for establishing and managing Air Force COTS software licenses and ensuring compliance with

The Copyright Act and E.O. 13103. It also complies with *The Information Technology Management Reform Act* (Division E of Public Law 104-106), and eliminates the Ada waiver process. Using Ada software programming language is no longer mandatory. Revised **Attachment 2** and removed Attachment 3. This revision makes AF Form 1375, **Data Systems Authorization Directory (DSADS) Request**, obsolete. The (I) preceding the publication title indicates a major revision from the previous edition.

Section A	Introduction	4
1.	Purpose	4
2.	Objectives	4
Section B	Responsibilities	4
3.	Headquarters United States Air Force Directorate of Communications and	4
4.	Major Command (MAJCOM), Direct Reporting Unit (DRU), Field Oper	4
5.	Headquarters Air Force Communications Agency	5
6.	Headquarters Air Force Materiel Command	5
7.	Headquarters Air Education and Training Command	5
8.	Individual Commercial Off-The-Shelf Software Users	5
Section C	Installation-Level Software Management	6
9.	Managing Licensed Commercial Off-The-Shelf Software	6
9.	(910AW) Managing Licensed Commercial Off-The-Shelf Software:	6
10.	Software Developed Using Commercial Off-The-Shelf Office Software	8
11.	Command, Control, Communications, Computers, and Intelligence (C4I)	8
12.	Configuration Management	9
13.	Information Assurance	9
14.	Open Systems Guidelines	10
15.	Software Reuse	10
16.	Data Administration	10
17.	Bandwidth	10
18.	Checklists	11
Attachment 1—GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION		12
Attachment 2—RELEASE OF SOFTWARE		16
Attachment 3—(Added-910AW) SAMPLE OF INVENTORY SHEET		19
Attachment 4—(Added-910AW) NETWORK FOLDER		20

AFI33-114_910AWSUP1_I 1 OCTOBER 2001	3
Attachment 5—(Added-910AW) TOTAL SOFTWARE LIST BY CSSOS OR COMPUSEC MANAGERS	21
Attachment 6—(Added-910AW) TOTAL BASE-WIDE INVENTORY SHEET	22
Attachment 7—(Added-910AW) CHANGE OF STATUS WORKSHEET	23
Attachment 8—(Added-910AW) ANNUAL INVENTORY MEMORANDUM	24

Section A—Introduction

1. Purpose . This instruction provides the guidance and procedures that personnel must use to plan, develop, use, maintain, or support Air Force software to effectively and efficiently complete their assigned missions. It applies to Air Force-procured COTS software and software developed for unique Air Force purposes (other than software internal to a weapon system; see AFPD 63-1). Maintain and dispose of records created as a result of the processes described in this instruction in accordance with AFMAN 37-139, *Records Disposition Schedule* (will convert to AFI 33-322 Volume 4 [AFI 33-322V4]).

2. Objectives .

- 2.1. Gives commanders and users of software at all levels guidance for managing licensed and other software used by Air Force personnel.
- 2.2. References requirements for standardizing documentation and implementation processes.

Section B—Responsibilities

3. Headquarters United States Air Force Directorate of Communications and Information (HQ USAF/SC).

- 3.1. Establishes and oversees computer software management regulatory and policy guidelines.
- 3.2. Implements Federal Chief Information Officers Council's recommendations for Air Force acquisition and use of computer software, and monitoring and combating the use of unauthorized computer software.
- 3.3. Ensures compliance with DoDD 8320.1, *DoD Data Administration*, September 26, 1991.

4. Major Command (MAJCOM), Direct Reporting Unit (DRU), Field Operating Agency (FOA), and Organizational Commanders.

- 4.1. All MAJCOM/DRU/FOA communications and information systems officers (CSO), where assigned, or commanders representatives where not assigned, will:
 - 4.1.1. Conduct and document an annual inventory of licenses as required by E.O. 13103.
 - 4.1.2. Establish a process to track licenses (see paragraph **9**).
 - 4.1.3. Develop performance measurements and metrics for software license requirements as required by E.O. 13103.
 - 4.1.4. Identify enterprise software license requirements and management training requirements not covered in existing courses to HQ AFCA for annual consolidation.
- 4.2. Compare licensing purchasing options including analysis of an enterprise-wide COTS software license as an option for satisfying COTS software requirements.
- 4.3. Plan and budget for support of software licenses and unique mission software through the information systems life cycle and arrange for software support at deployment locations, when needed.

4.4. Obtain COTS software under Department of Defense (DoD)-wide and Air Force enterprise licenses rather than individual client or server purchases. Accomplish comparative analysis of enterprise licenses purchase opportunities to ensure Air Force receives the best value. Coordinate with the host communications unit or servicing Network Control Center before making any software purchases.

5. Headquarters Air Force Communications Agency .

5.1. Surveys and consolidates MAJCOM, FOA, and DRU requirements for potential Air Force enterprise software licenses for COTS computer and network management software.

5.2. Recommends candidate software products for potential Air Force-wide licensing to the Air Force Materiel Command (AFMC) product center designated with the responsibility for enterprise license management.

5.3. Consolidates new MAJCOM training for managing software licenses (including computer-based initiatives) and sends them to Headquarters Air Education and Training Command (HQ AETC/SCX, 61 Main Circle Suite 2, Randolph AFB TX 78150-4545) for incorporating formal courses or in long-distance learning approaches.

6. Headquarters Air Force Materiel Command .

6.1. Designates a product center as the office of primary responsibility (OPR) for managing the Air Force Enterprise Software License Program and, when designated, acts as executive agent for establishing DoD-wide enterprise software licenses.

6.2. Designates a product center as purchasing agent for software licenses to support consolidated and programmatic Air Force requirements.

6.3. Manages Air Force Enterprise Software Licenses for COTS computer and network management software.

7. Headquarters Air Education and Training Command .

7.1. Develops training plans and materials for comprehensive training that addresses all aspects of managing the operation of installation-level licensed software.

7.2. Establishes curricula for formal licensed software management courses identified by HQ AFCA/ITC in coordination with Headquarters Air Force Communications and Information Center (HQ AFCIC/ITA).

7.3. Provides training through centrally managed computer based training courses or other distance learning approaches.

8. Individual Commercial Off-The-Shelf Software Users .

8.1. 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 base CSO has authorized such use. When authorized for installation on a home computer, only use the software for official Air Force business. Personal use may be a violation of *The Copyright Act*, rendering the individual user accountable and liable.

- 8.2. Do not install freeware, shareware, or personally owned software on government systems without approval of the system administrator or network manager servicing your organization, according to AFI 33-115V1, *Network Management*; and AFI 33-202, *Computer Security*.
- 8.3. Do not make any illegal copies of copyrighted software.

Section C—Installation-Level Software Management

9. Managing Licensed Commercial Off-The-Shelf Software . The communications squadron commander or CSO at each installation who implements licensed COTS or other software shall:

9. (910AW) Managing Licensed Commercial Off-The-Shelf Software: All 910 AW Workgroup Managers (WGMs), Computer Security (COMPUSEC) managers and Computer System Security Officers (CSSOs) who implement licensed COTS or other software shall ensure the following:

- 9.1. Develop and implement a documented process to ensure that all software (including freeware, shareware, licensed COTS products, and pre-production versions) is free of viruses and malicious logic.
- 9.2. Annually instruct personnel on licensed software usage; *The Privacy Act* and *The Copyright Act* considerations; and Air Force, DoD and E.O. provisions.
 - 9.2.1. (Added-910AW) Annual training in software management and software piracy is available to all users on the intranet information assurance page. The test will be graded, tracked and filed with the Wing Information Assurance Specialist.
- 9.3. Register organization ownership of licensed COTS software and ensure an annual inventory is conducted of all licensed COTS software in the organization.
 - 9.3.1. (Added-910AW) An annual inventory of all computer systems will be conducted between April 1 and April 30 by the COMPUSEC manager or CSSO using System Management Server (SMS) on network machines. The COMPUSEC manager or CSSO will have to conduct a manual inventory on non-network computers and on extra drives on all computers (format shown in [Attachment 1](#)).
 - 9.3.2. (Added-910AW) Periodic spot checks of inventoried machines will be conducted by the Software Manager and WGM using SMS. The WGM will randomly sample machines bimonthly. Any discrepancy will be reported to the Software Manager for review and further action to be taken if necessary.
 - 9.3.3. (Added-910AW) The WGM will remove all unauthorized software upon discovery.
- 9.4. Use a metering mechanism if licensed for server-hosted, concurrent-user application software to prevent exceeding the authorized number of copies and users. Record network manager or system administrator inventory of licensed client and network software as part of the annual installation licensed software inventory.
- 9.5. Maintain a record of the COTS software controlled by the organization.
 - 9.5.1. (Added-910AW) The Software Manager and WGM will maintain an inventory of all software and ensure that a license or other proof of legal use is available. A soft copy of the inventory will be kept on the network for ease of access. The Software Manager must be notified of any

changes made to the files kept on the network by sending a change of status form. (See [Attachment 2-Attachment 5 \(Added-910AW\)](#).)

9.5.2. (Added-910AW) The COMPUSEC manager or CSSO will sign a memorandum stating that an annual inventory was completed. (See [Attachment 6 \(Added-910AW\)](#).)

9.6. Store evidence (e.g., user manual, purchase documentation, compact disk, etc.) of licenses in a secure location (e.g., a locked file cabinet).

9.6.1. (Added-910AW) The COMPUSEC manager or CSSO will ensure that all computer users have proof of the authority to use the software loaded on the computer. Proof may be original disks, receipts with serial numbers, site licenses, proof of registration provided by the software company, or the location of this proof. This is the case for copyrighted software that the Air Force has rights to use (i.e., software provided without restrictions to the Air Force or where an Air Force-wide site license is in force.)

9.6.2. (Added-910AW) All authorized licensed software will be stored by the COMPUSEC manager or CSSO in a secure location and labeled appropriately.

9.7. Dispose of old versions of COTS software according to licensing agreements. Upgrades from the original software source are normally considered a continuation of the original license, not an additional or new license.

9.8. Redistribute excess or superseded COTS software if it:

9.8.1. Is allowed under the license agreement or upgrade policy for that software.

9.8.2. Is not classified.

9.8.3. Did not provide direct security protection to automated data processing equipment in systems that processed classified information.

9.8.4. Is not directly related to or associated with a weapon system, intelligence system, command and control system, communications system, or tactical system.

9.8.5. Still operates as intended.

9.9. Dispose of excess or superseded COTS software not redistributed by one of the following methods:

9.9.1. Return the software package (distribution media, manuals, etc.) to the company that developed the software.

9.9.2. Destroy the software according to the provisions of the licensing agreement. (**NOTE:** Document the method of destruction to establish an audit trail.) This may include:

9.9.2.1. Destroying the documentation and distribution media.

9.9.2.2. Formatting or erasing the master floppy disks.

9.9.2.3. Using the master floppy disks as scratch disks.

9.9.3. Audit all computer and server software annually to ensure there are no illegal or unauthorized copies of COTS or other software installed. Sampling procedures may be used if active inventorying is available.

10. Software Developed Using Commercial Off-The-Shelf Office Software Tools. Air Force computer users are encouraged and expected to use their licensed COTS office software to increase their individual professional productivity and overall unit effectiveness. Users must coordinate networked or “group” computer applications that are user built with these tools with the installation CSO. This precludes later impact on network and server capacity, avoids duplication of effort on similar application software within the installation or MAJCOM, and ensures continued software support after departure of one or more of the original user-developers. Air Force user-developers shall:

10.1. Ensure the Air Force retains property rights to the computer software developed in the course of their duties.

10.2. Not by-pass computer/network server operating systems, security systems, or access controls provided by higher authority.

10.3. Provide the CSO a software documentation package in appropriate digital format. The software package must include:

10.3.1. The author or point of contact, organization, and telephone number.

10.3.2. A descriptive unclassified title with version number as the first delivery (use Version 1.0).

10.3.3. A brief (one paragraph) unclassified description of the software’s functionality for use in publishing software reuse catalogs; and a classified description, if necessary, to more fully explain the software’s capabilities.

10.3.4. A brief description of all testing (such as Year 2000) performed on the mission application software and its databases.

10.3.5. A brief user’s guide. The user’s guide should include:

10.3.5.1. The hardware configuration required.

10.3.5.2. The supporting software required to include the operating system and (if any) supporting COTS software with version release number.

10.3.5.3. Compiling and linking instructions, if applicable.

10.3.5.4. Descriptions of the software installation process, required hardware setup, menus, and software capabilities and functions.

10.3.5.5. Samples of terminal output screens and print products produced (if any).

10.3.5.6. Other information useful for continued effective use and maintenance of the mission application software.

11. Command, Control, Communications, Computers, and Intelligence (C4I) Software Development; Reuse; and Release. Adhere to DoDD 3405.1; DoDD 4630.5, *Compatibility, Interoperability, and Integration of Command, Control, Communications, and Intelligence (C3I) Systems*, November 12, 1992; DoD Instruction (DoDI) 4630.8, *Procedures for Compatibility, Interoperability, and Integration of Command, Control, Communications, and Intelligence (C3I) Systems*, November 18, 1992; and Chairman Joint Chiefs of Staff Instruction (CJCSI) 6212.01A, *Compatibility, Interoperability, and Integration of Command, Control, Communications, Computers, and Intelligence Systems*, 30 June 1995; when developing mission or application software for C4I systems.

11.1. Organic Development. Do not develop software organically unless quality, cost, performance, schedule, or interoperability requirements cannot be met with COTS or non-developmental item software.

11.1.1. Acquire an approved mission needs statement before developing organic software requiring over 6 man-months of effort or costing in excess of \$50,000, and follow guidance for software acquired under DoD 5000-series acquisitions.

11.1.2. All units that develop or maintain software will have a software process improvement (SPI) program and a documented SPI plan, including at least:

11.1.2.1. A baseline of their current capabilities.

11.1.2.2. Goals and milestones they intend to reach.

11.1.2.3. Metrics to measure their progress toward their goals and milestones.

11.1.2.4. Timeline for SPI appraisals. The Software Technology Support Center (STSC) at Hill Air Force Base UT is available on a fee-recovery basis for SPI appraisals, but any qualified SPI appraiser may be used.

11.1.2.5. Identify life-cycle support requirements for the life of developed software.

11.2. Releasing COTS Office Software Tools. It is Air Force policy to release, upon consideration of a valid written request, specific software developed exclusively with government funds or otherwise owned by the Air Force. The OPR for the software decides to release or disclose that software. The approval authority may be at a higher level depending upon the recipient (e.g., approval authority for all foreign release requests is Secretary of the Air Force [SAF/IADD]). When not for foreign release and the OPR is in doubt regarding the release of software, send the request to HQ USAF/SCX, 1250 Air Force Pentagon, Washington DC 20330-1250, for resolution. *Freedom of Information Act* (FOIA) requests must be sent to the local FOIA manager to control and respond using guidelines in the Air Force supplement to DoD 5400.7-R (DoD 5400.7-R/AFSUP), *DoD Freedom Of Information Act Program*, 22 July 1999. Before releasing the software, the OPR shall require the requester to sign a memorandum of agreement (see [Attachment 2](#)). Releases of Air Force-owned or developed software from software reuse libraries, or software under Air Force-industry Cooperative Research and Development Agreements (CRADA), are exceptions to this policy.

12. Configuration Management . Define and manage the configuration of computer software according to commercial standards (i.e., those developed by the International Standards Organization, American National Standards Institute, or Institute of Electrical and Electronic Engineers, and best practices advocated by the Software Engineering Institute, and the STSC at Hill AFB UT).

13. Information Assurance . Program managers and software developers must integrate information assurance into their systems using guidance contained in AFD 33-2, *Information Protection* (converting to *Information Assurance*); the Air Force 33-200 series publications; and Air Force systems security instructions and memoranda listed in Air Force Index (AFIND) 5, *Numerical Index of Specialized Information Protection Publications*. These publications give policy guidelines for developing and using the computer, communications, and emissions security programs needed for all Air Force communications and information systems.

14. Open Systems Guidelines . The Air Force is committed to meeting the DoD objective of developing interoperable and maintainable systems based on open standards. To that end, system developers, contract administrators, and maintainers must adhere to the guidance given in the DoD Joint Technical Architecture (JTA) and JTA-Air Force (JTA-AF). These documents identify a common set of mandatory information technology standards and guidelines used in all new systems and system upgrades in the DoD. Each unit ensures that upgrades to systems under maintenance comply to the maximum extent possible with the JTA and JTA-AF.

15. Software Reuse . Software reuse is the practice of using existing software components to develop new software applications. Software reuse benefits the Air Force through increased developer productivity, improved quality and reliability of software-intensive systems, enhanced system interoperability, lowered program technical risk, and shortened software development and maintenance time.

15.1. Reusable software components may include executable software binaries, source code segments, program documentation, project plans, requirement descriptions, design and architecture documents, database schemas, test data and test plans, user's manuals, software tools, and object classes. These assets can be most efficiently used when designed and packaged to fit into a product-line architecture at each software development location for a specific mission area or functional domain, using interface standards and common communications protocols. The domain product-line components can then be used to create families of related systems designed to share common software architecture for the domain.

15.2. Each Air Force software development location should:

15.2.1. Establish a software reuse library or repository for internal sharing of the reusable software components developed at the location.

15.2.2. Report each reusable software component to the Air Force Reuse Center, Standard Systems Group, Maxwell AFB-Gunter Annex AL, for storage in the Air Force Defense Software Repository System.

15.2.3. Upon valid written request, release software component using the software release memorandum of agreement at [Attachment 2](#).

16. Data Administration . All Air Force organizations developing software or overseeing software development contracts follow the guidelines published in AFI 33-110, *Data Administration Program*; DoDD 8320.1; DoD 8320.1-M, *Data Administration Procedures*, March 29, 1994; and DoD 8320.1-M-1, *Data Standardization Procedures*, April 2, 1998. Contact HQ AFCA/ITC for additional guidance.

17. Bandwidth . The Air Force is faced with restrictions on the amount of information that can be provided to our forces, particularly in remote areas of the world. Therefore, software systems designers and developers must discipline themselves in the quantity and content of non-mission essential information sent over supporting network infrastructures (that is, ensure sending only operationally necessary data). In addition to DoD direction, follow all policy and procedures in AFIs 33-101, *Communications and Information Management Guidance and Responsibilities*; 33-115V1; 33-119, *Electronic Mail (E-Mail) Management and Use*; and 33-129, *Transmission of Information Via the Internet*; on downloading from the Internet, transmission of e-mail attachments, video teleconferencing, Web browsing, and conservation measures during periods of surge or network degradation. Air

Force-developed software (including that developed specifically for the Air Force) will accommodate network infrastructure considerations into its systems design and internal code, such that it does not overtax the infrastructure that it relies and operates.

18. Checklists . Use AF Form 2519, **All Purpose Checklist** (available electronically), to develop a checklist on software and software license management using paragraphs **3.** through **8.**

GARY A. AMBROSE, Brig General, USAF
Acting Director, Communications and Information

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

E.O. 13103, *Computer Software Piracy*, September 30, 1998

Freedom of Information Act

The Copyright Act

The Information Technology Management Reform Act (Division E of Public Law 104-106)

The Privacy Act

CJCSI 6212.01A, *Compatibility, Interoperability, and Integration of Command, Control, Communications, Computers, and Intelligence Systems*, 30 June 1995

DoDD 3405.1, *Computer Programming Language Policy*, April 2, 1987

DoDD 4630.5, *Compatibility, Interoperability, and Integration of Command, Control, Communications, and Intelligence (C3I) Systems*, November 12, 1992

DoDI 4630.8, *Procedures for Compatibility, Interoperability, and Integration of Command, Control, Communications, and Intelligence (C3I) Systems*, November 18, 1992

DoD 5400.7-R/AFSUP, *DoD Freedom of Information Act Program*, 22 July 1999

DoDD 8320.1, *DoD Data Administration*, September 26, 1991

DoD 8320.1-M, *Data Administration Procedures*, March 29, 1994

DoD 8320.1-M-1, *Data Standardization Procedures*, April 2, 1998

AFIND 5, *Numerical Index of Specialized Information Protection Publications*

AFI 21-116, *Maintenance Management of Communications-Electronics*

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

AFPD 33-2, *Information Protection (converting to Information Assurance)*

AFI 33-101, *Communications and Information Management Guidance and Responsibilities*

AFI 33-110, *Data Administration Program*

AFI 33-115V1, *Network 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*

AFDIR 33-303, *Compendium of Communications and Information Terminology*

AFMAN 37-139, *Records Disposition Schedule (will convert to AFI 33-322V4)*

AFPD 63-1, *Acquisition System*

Information Security Products Catalog, published annually and updated quarterly by the National Security Agency, gives evaluation information on computer security (COMPUSEC), cryptographic, emission-tested security, and destruction equipment.

Air Force Assessed Products List, available on the HQ AFCA/GCI home page, gives information on COMPUSEC system and subsystem assessments requested by Air Force users.

Abbreviations and Acronyms

AFI—Air Force Instruction

AFIND—Air Force Index

AFMC—Air Force Materiel Command

AFPD—Air Force Policy Directive

C4—Command, Control, Communications, and Computers

C4I—Command, Control, Communications, Computers, and Intelligence

CJCSI—Chairman Joint Chiefs of Staff Instruction

COMPUSEC—Computer Security

COTS—Commercial Off-the-Shelf

CRADA—Cooperative Research and Development Agreements

CSO—Communications and Information Systems Officer

DoD—Department of Defense

DoDD—Department of Defense Directive

DoDI—Department of Defense Instruction

DRU—Direct Reporting Unit

E.O.—Executive Order

FOA—Field Operating Agency

FOIA—Freedom of Information Act

HQ AETC—Air Education and Training Command

HQ AFCA—Air Force Communications Agency

HQ AFCIC—Air Force Communications and Information Center

HQ USAF—Headquarters United States Air Force

JTA—Joint Technical Architecture

JTA-AF—Joint Technical Architecture-Air Force

MAJCOM—Major Command

OPR—Office of Primary Responsibility

SAF—Secretary of the Air Force

SPI—Software Process Improvement

STSC—Software Technology Support Center

Terms

Certification—For purposes of this instruction, the act of determining that software performs without defects and viruses, and does what the supporting documentation says it will do in accordance with any specified acceptance criteria.

Command, Control, Communications, and Computer (C4) Systems—Integrated systems of doctrine, procedures, organizational structures, personnel, equipment, facilities, and communications designed to support a commander's exercise of command and control, across the range of military operations. Also called "communications and information systems."

Commercial Off-The-Shelf (COTS) Software—Software developed, tested, and sold by commercial companies to the general public. Examples include word processors, databases, application generation, drawing, compiler, graphics, communications, and training software.

Communications and Information Systems Officer (CSO)—Identifies the supporting CSO at all levels. At base level, this is the commander of the communications unit responsible for carrying out base communications and information systems responsibilities, the base CSO. Tenant organizations may also have CSOs. At MAJCOM, and other activities responsible for large quantities of communications and information assets, it is the person designated by the commander as responsible for overall management of communications and information assets budgeted and funded by the MAJCOM or activity. The CSO function, when under the base communications unit, uses the office symbol "SC" that expands to three and four digits to identify specific functional areas.

Computer Security (COMPUSEC)—1. The protection resulting from all measures to deny unauthorized access and exploitation of friendly computer systems. See also "communications security".
2. Measures and controls that ensure confidentiality, integrity, and availability of information systems assets including hardware, software, firmware, and information being processed, stored, and communicated.

Copyright—Without a license that specifies otherwise, the purchaser's use of software is restricted to making an archival copy and installing the computer program onto a single computer, in accordance with the *Copyright Act of 1976*. Do not reproduce or use copyrighted software in any other manner.

Documentation—Records required to plan, develop, operate, maintain, and use electronic records and software. Included are systems specifications, file specifications, code books, record layouts, user guides, and output specifications.

Hardware—The physical equipment and devices forming a computer and peripheral components.

Interoperability The ability of systems, units, or forces to provide services to and accept services from other systems, units, or forces and to use the services so exchanged to enable them to operate effectively together. The condition achieved among communications-electronics systems or items of communications-electronics equipment when exchanging information or services directly and satisfactorily between them and/or their users.

License Agreements—Contracts between the software publisher and the user that instruct and limit the software use. When purchasing software, the buyer only acquires a license to use it. The publisher retains

the full rights to the software and has the sole right to its further distribution and reproduction.

Maintenance—Any job described as one that eliminates faults or keeps hardware or software running in satisfactory working condition falls into the maintenance category. (See AFI 21-116, *Maintenance Management of Communications-Electronics*.)

Network—Two or more computers connected to each other through a multi-user system or by other electronic means to exchange information or share computer hardware or software.

Requirement—A need for a new or improved information processing capability that, when satisfied, increases the probability of operational mission success or decreases the cost of mission support.

Reuse—The process of developing or supporting a software intensive system using existing software assets. (See DoDD 3405.1.)

Sensitive Information—The loss, misuse, unauthorized access to, or modification of information that could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under Title 5 U.S.C. Section 522a (*The Privacy Act*), but that has not been specifically authorized under criteria established by an E.O. or an Act of Congress to be kept SECRET in the interest of the national defense or foreign policy. (See Air Force Directory [AFDIR] 33-303, *Compendium of Communications and Information Terminology*.)

Shareware—Privately or commercially developed software that users receive free of charge but pay a fee for continued or extended use. Normally, implied or promised support by the author is minimal or nonexistent. (See AFDIR 33-303.)

Software—A set of computer programs, procedures, and associated documentation concerned with the operation of a data processing system (for example, compilers, library routines, and manuals).

User—The individual who operates the computer or uses application software.

Attachment 2

RELEASE OF SOFTWARE

A2.1. Software Reuse . It is HQ USAF policy to consider releasing specific software upon receiving a valid written request.

A2.1.1. Software is available from the Central Archive for Reusable Defense Software, the Defense Software Repository System, or the Air Force Defense Software Repository System. In such releases, the memorandum of agreement at paragraph **A2.3.** need not be completed.

A2.1.2. As government furnished property software is available under the provisions of an acquisition contract. **NOTE:** When the government has unlimited rights in computer software in the possession of a contractor, the government will not pay for the use of such software in performance of government contracts or for the later delivery to the government of such computer software, provided that the contractor be entitled to compensation for converting the software into the prescribed form for reproduction and delivery to the government. In addition to adhering to the specific contract's provisions, the contractor also must sign the memorandum of agreement at paragraph **A2.3.**

A2.1.3. Software is also available to organizations with which the Air Force does not have a contractual arrangement. In such situations, the recipient must sign the memorandum of agreement at paragraph **A2.3.**

A2.2. Software Release or Disclosure . Each OPR bases the decision to release or disclose software on review of all significant factors including but not limited to, national security, militarily critical technology/dual use, royalty arrangements, potential for Air Force-industry CRADA, or pre-existing license agreement terms and conditions.

A2.2.1. In all software releases, the Air Force must ensure that it will not be held liable for any failure of the released software or its continued maintenance. This also applies to Air Force software deposited in all software reuse libraries. As such, the OPR must ensure that recipients of software from the reuse libraries understand this waiver of warranties and damages liability.

A2.3. Memorandum of Agreement :

I/We the undersigned, on behalf of the Requesting Organization listed below (hereafter referred to as the "Requester"), request release of (software name) and understand and agree to the following:

a. NON-DISCLOSURE AGREEMENT. The Requester requests some or all of the following from _____ (insert the name of the specific Air Force organization or software reuse library): data, technical data, computer software, computer software documentation, computer programs, source code, firmware, and other information of like kind, type, or quality, either commercial or non-commercial, all of which may be subject to limited rights, restricted rights, government-purpose license rights, patents, copyrights, trade secret rights, or other confidential or proprietary constraints (collectively, the "Data"). In consideration therefore, the Requester agrees:

- 1) That the Data shall be used only for government, non-commercial, or non-profit purposes.

2) To strictly abide by and adhere to any and all restrictive markings placed on the Data, and the Requester shall not knowingly disclose or release the Data to third parties who are not engaged in work related to government, non-commercial, or non-profit purposes.

3) That any restrictive markings on the Data shall be included on all copies, modifications, and derivative works, or any parts or portions thereof; in any form, manner or substance, which are produced by the Requester including but not limited to incorporation of the Data into any other data, technical data, computer software, computer software documentation, computer programs, source code, or firmware, or other information of like kind, type or quality. In all such events, Requester shall clearly denote where such Data initiates and concludes by use of annotations or other standard markings.

4) That the government is entitled to royalty-free use of the Air Force-owned or -developed software that is released.

b. WAIVER OF WARRANTIES AND LIMITATIONS OF DAMAGES AGREEMENT. The requester and the Approving Authority agree that:

1) No guaranties, representations, or warranties either expressed or implied shall be construed to exist in any language, provision, or term contained in these materials or in any other documentation provided herewith (all such items are collectively referred to as the "Agreement"), and furthermore, the releasing organization disclaims and the requester waives and excludes any and all warranties of merchantability and any and all warranties of fitness for any particular purpose.

2) The Requester shall obtain from the releasing organization all of the "Data" (defined in the Non-Disclosure Agreement above), or any other products or services contemplated by the Agreement, in an "as is" condition.

3) The Requestor agrees to hold harmless and indemnify the Air Force against any and all loss, liability, cost or expense arising out of the use of any Data released under this agreement, to include, but not limited to, litigation costs or expenses.

c. The Requester's use of the Data shall not prevent the government from releasing the Data at any point in the future.

d. The Requester shall not offer the released Data or any modified version thereof for resale to the government, in whole or as part or subpart of a government deliverable, without explicitly stating that he is doing so by providing certification documentation (e.g., Section K of the Government Solicitation) to the contracting officer before contract award.

e. The Requester may use the released Data in a contract with the government, but understands that the government shall not pay the Requester for rights of use of such Data in performance of government contracts or for the later delivery to the government of such Data. The Requester may be entitled to compensation for converting, modifying, or enhancing the Data into another form for reproduction and delivery to the government, if authorized under a contract with the government.

f. The Requester is not entitled to any released Data that are subject to national defense security classification or the proprietary rights of others. The Requester shall report promptly the discovery of any such restricted Data to the USAF release approving authority below, and follow all instructions concerning the use, safeguarding, or return of such Data. The Requester shall not copy, or make future study or use of any released Data later found to be subject to such restrictions.

g. As required, the Requester shall be responsible for compliance with any proscriptions on foreign disclosure of the released Data (contained, for example, in the Department of State International Traffic in Arms Regulations or the Department of Commerce Export Administration Regulations).

h. There may be a fee to cover the copying and shipping of the Data and any documentation.

i. The Requester and the Approving Authority intend that all agreements under this Memorandum of Agreement shall be governed by the laws of the United States of America.

NAME OF REQUESTOR

NAME/TITLE OF USAF APPROVING AUTHORITY

Requesting Organization/Address

Air Force Organization/Address

City, State, Zip Code

City, State, Zip Code

Signature of Requestor and Date

Signature of USAF Approving Authority and Date

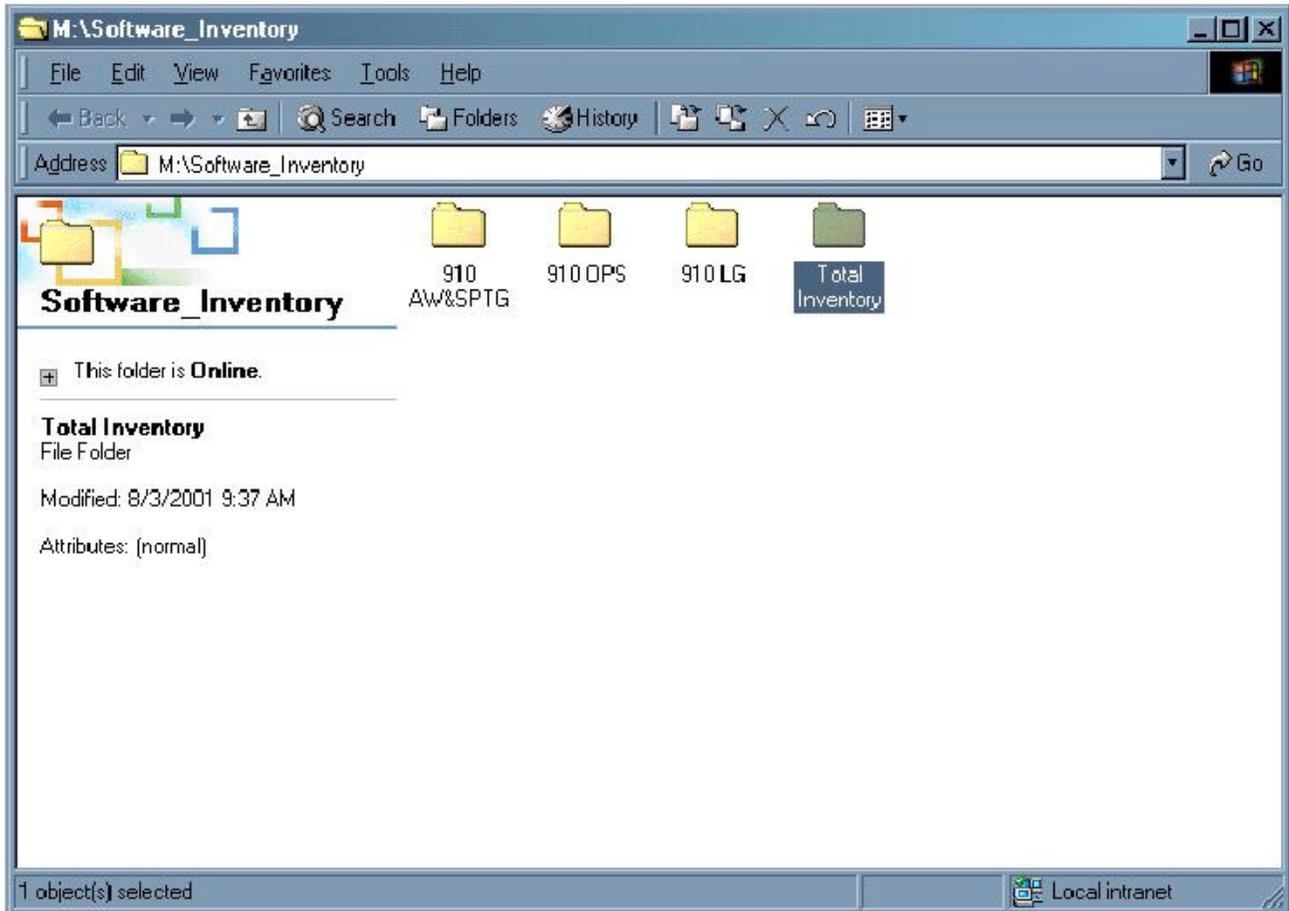
Attachment 3 (Added-910AW)

SAMPLE OF INVENTORY SHEET

A3.1. (Added-910AW) Inventory Sheet.

SOFTWARE TITLE	Total Count	SOFTWARE TITLE
AccessRamp (Inverse Network Technology)	1	Microsoft Windows 2000 OS
Adaptec CD Jewel*	15	Microsoft Windows NT 4.0 for workstations
Adaptec DirectCD*	19	Mjuice Media Player(freeware)
Adaptec Easy CD Creator*	18	MusicMatch (licensed)
Adaptec UDF Reader*	19	MusicMatch***
Adobe Acrobat (5.0) (licensed)	2	MyCD (freeware)
Adobe Acrobat Reader (3.0) (freeware)	2	MyCorkboard (PC Dynamics)
Adobe Acrobat Reader (4.0) (freeware)	30	NAB Conduit Install Application(Fishbone)
Adobe Acrobat Reader (5.0) (freeware)	2	Napigator (Thirty4 Interactive LLC)
Adobe Acrobat Reader for Palm OS (freeware)	1	Nere-Burning Rom (ahead software)
Adobe Illustrator (9.0)*** (licensed)	1	NetPlus WinSNMP/32 (licensed)
Adobe Image Ready (2.0)***	1	Netscape (Network install)
Adobe Image Ready (3.0)***	1	Netscape 4.7 (network install is 4.61)
Adobe PhotoDeluxe Business Edition(5.0)*** (licensed)	2	nFX Cartoon.O-Matic
Adobe Photoshop (5.0)*** (licensed)	1	Nikon View (FotoNation Inc)
Adobe Photoshop (6.0)*** (licensed)	1	Norton Anti-Virus (7.01-7.5)(network install)****
Aforms Reports (Air Force)	1	Norton LiveUpdate (network install)
Airforce (Air Force?)	1	Norton Systemworks
AKSoft (freeware)	2	Norton Utilities

Each computer inventory is a separate spreadsheet.
 The above is a sample of a total sheet of all the computers and what is currently on them.
 Any software that is bold (red) means that the CSSO must verify that the software is a legal version. If it is not then the software will be removed from the computer in question by the WGM.

Attachment 4 (Added-910AW)**NETWORK FOLDER****A4.1. (Added-910AW) Network Folder.**

The software inventory folder is found on the M drive under WGM's groups. The Total Inventory folder is used by the Software Manager and WGM's for totaling the entire base software inventories.

Attachment 5 (Added-910AW)

TOTAL SOFTWARE LIST BY CSSOS OR COMPUSEC MANAGERS

A5.1. (Added-910AW) Total Software.

SOFTWARE LIST			
CSSO		Michelle West Group	
SOFTWARE TITLE	Totals	SOFTWARE TITLE	Totals
3COM DynAcc ver 1.5	3	Norton Antivirus	21
3COM Diagnostics*	12	Nova Disk ver 6.6 *	1
3COM Family Media Kit	5	NTI CD Maker Pro (included w/system)	1
3D Sound Express	1	Oracle for Windows (no license)	1
ADC (Air Force)	1	ORM Training (Air Force)	2
Adobe Acrobat 3.0 (shareware)	7	Outlook Express (Include w/explorer)	20
Adobe Acrobat 4.0 (shareware)	15	PARIS Viewer (Freeware)	1
Adaptect Direct CD	5	RCSBP Calculator (freeware)	1
Adaptect CD Creator	5	Realplayer (freeware)	7
Adaptect UD Reader	1	Real3D Starfighter AGP	1
AFEMIS (Air Force)	5	SCM Card wizard	4
AFRCEPL (Air Force)	1	Softex (docking software)	1
Asnud (Air Force)	3	Sound MAX WDM *	2
Argus PCI Interface	1	SMAS OSE (Air Force)	1
CBT (Air Force)	2	Swapbox PCI Reader	3
CD Audio System	1	Thud	2
Comet Cursor (freeware)	4	UBS Supp to OSR2 *	2
CPS (Air Force)	3	VBS Ctrl Creation Ed	1
Dell OpenMg. Client	11	VDOLive Player *	12
Design XP Label Maker (included w/system)	1	VIDIA Video Driver	5

Each CSSO or COMPUSEC manager will have a total page (one Excel file for each WGM.)
 Template is used as a starting point for each total page.

Attachment 6 (Added-910AW)

TOTAL BASE-WIDE INVENTORY SHEET

A6.1. (Added-910AW) Total Base Wide Inventory.

The screenshot shows a Microsoft Excel spreadsheet titled "Total Inventory". The spreadsheet is divided into two main sections. The first section, starting at row 1, is titled "Total Commercial Software Inventoried" in blue text. It has a header row (row 2) with columns: Software Title (A), LG Group (Dale) (B), OPS Group (Kathy) (C), 910 AW& STPG(Chuck) (D), Total Amount (E), and Total Amount Licensed (F). The second section, starting at row 16, is titled "Total Freeware/Shareware Software Inventoried" in blue text. It has a header row (row 17) with columns: Software Title (A), LG Group (Dale) (B), OPS Group (Kathy) (C), 910 AW& STPG(Chuck) (D), Total Amount (E), and Total Amount Licensed (F). The spreadsheet interface includes a menu bar (File, Edit, View, Insert, Format, Tools, Data, Window, Help), a toolbar with various icons, and a status bar at the bottom showing "Ready" and "NUM".

↑ Total Air Force Software Sheet
↑ Commercial Software Total Sheet
↑ WGM's Group Totals Sheet

Attachment 8 (Added-910AW)**ANNUAL INVENTORY MEMORANDUM****A8.1. (Added-910AW) Annual Inventory Memorandum.****DEPARTMENT OF THE AIR FORCE**
Air Force Reserve Command

Date

MEMORANDUM FOR 910 CF/SCI**FROM:** 910 (appropriate office symbol/organization)**SUBJECT:** Annual Software Inventory Compliance Certification

1. Per AFI 33-114/910 AW SUP, all appointed Computer Security Managers (COMUSEC Managers) or Computer System Security Officers (CSSOs) are required to conduct an annual software inventory for their area of responsibility.
2. The COMPUSEC Manager or CSSO signature on this document certifies that the software inventory for the computer equipment custodians (EC) was conducted and all software is accounted for.
3. Listed below is the name of the appointed COMPUSEC Manager or CSSO and the EC accounts where the inventories were conducted.

COMPUSEC Manager or CSSO:

EC Account(s) of Responsibility:

4. I certify that the above listed EC accounts have been inventoried and all software is accounted for:

CSSO Name and Title

EXAMPLE