OFFICE OF THE SECRETARY OF DEFENSE

WASHINGTON D.C. 20301

APR 8, 1997

MEMORANDUM SECRETARIES OF THE MILITARY DEPARTMENTS
VICE CHAIRMAN, JOINT CHIEFS OF STAFF
ASSISTANT SECRETARY OF DEFENSE (COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE)

SUBJECT: Guidelines on International Transfers of Software Documentation (including Source Code)

The Department of Defense will give favorable consideration to requests for transfers of software documentation (including source code) consistent with national security interests and applicable laws, regulations, policies, and international agreements. DOD's review of software documentation transfers will be on a case-by-case basis through established internal review mechanisms in accordance with the attached "Department of Defense Guidelines for International Transfers of Software Documentation (including Source Code)."

The members of the Senior Working Group and their staffs who developed these guidelines are to be congratulated for a job well done.

/s/
R. Noel Longuemare
Principal Deputy Under
Secretary of Defense for
Acquisition and Technology

/s/
Jan M. Lodal
Principal Deputy Under
Secretary of Defense for
Policy

DEPARTMENT OF DEFENSE GUIDELINES FOR INTERNATIONAL TRANSFERS OF SOFTWARE DOCUMENTATION (including Source Code)

OBJECTIVE: To establish Department of Defense (DoD) wide guidelines for the development of DoD recommendations or decisions on international transfers of software documentation (including source code).

BACKGROUND: It is U.S. Government (USG) law and policy to transfer defense articles and services (including software) when such transfers will strengthen the security of the United States; help allies and friends deter or defend themselves against aggression while promoting interoperability with U.S. forces; and ensure that U.S. military forces continue to enjoy technological advantages over potential adversaries.

Software has become an integral and virtually ubiquitous part of U.S. military capabilities both in military operations and in the design, development, production, and operation of military systems, subsystems, and munitions. Software (including source code) used in military applications may contain national security information ranging from the routine to the highly sensitive depending on the *specific* military and intelligence applications for the software. Nothing in these guidelines supersedes or otherwise modifies the requirements of U.S. laws, regulations, or international agreements or arrangements to which the U.S. is a party (including prohibitions on transfers to specific destinations, or obligations of the USG). To the extent that the legal framework for transfers affords DoD discretion, these guidelines should be used to guide DoD recommendations or decisions.

CONTENT OF TRANSFER: All requests to transfer software documentation (including source code) must identify the specific information contained in the documentation that is proposed for transfer, and the specific end-user and end-uses for the documentation. If the proposed transfer requests for a system, subsystem, or other item that contains software does not specifically request the transfer of software documentation, the following standard limitation will be applied: "Because the transfer proposal did not request or address specific software documentation, no documentation may be transferred. Transfer of the software documentation must be the subject of a separate specific request."

TRANSFER GUIDELINES: DoD will give favorable consideration to requests for transfers of software documentation, on a case-by-case basis, through established internal review mechanisms consistent with applicable laws, regulations, policies, and international agreements, and consistent with the following guidelines. All recommendations by DoD reviewing organizations to deny or require conditions for proposed transfers will be accompanied by specific national security rationale supporting such recommendations.

(1) Favorable consideration will be given to the transfer of software documentation in support of end-items when all of the following have been appropriately addressed:

a) The recipient has purchased or committed to purchase the associated end-item in appropriate quantities relative to the recipient's inventory.

b) The recipient agrees to establish an appropriate level of indigenous software support for the end-item.

c) The recipient agrees to use the provided software documentation only for operation and support of the associated end-item.

d) The recipient acknowledges that system performance or warranties (when applicable) may be invalidated if changes are made to the software.

e) The risk of compromising critical DoD military capabilities, vulnerabilities, or intelligence data will not exceed the risk associated with end-item transfer, or any additional risk is offset by the benefit to the U.S. from the transfer of the software documentation.

(2) In support of designated international cooperative programs, DoD will give favorable consideration to transfers of software documentation (including source code) when:

a) A government-to-government agreement governs the program.

b) In the development of the government-to-government agreement, all of the guidelines in (1) above have been taken into account, as appropriate.

c) Recipient and U.S. responsibilities (e.g., support, maintenance and defect repair) are explicitly addressed as part of the government-to-government agreement.

(3) Favorable consideration will be given to the transfer of software documentation in support of production or development programs (e.g., technical and manufacturing assistance agreements) not governed by a government-to-government agreement when:

a) Guidelines (a) through (d) in (1) above have been taken into account, as appropriate.

b) Critical DoD military capabilities, vulnerabilities, or intelligence data will not be compromised, or the risk of compromise is offset by the benefit to the U.S. from the transfer of the software documentation.

FACTORS FOR CONSIDERATION: The DoD will consider the following factors together with the preceding guidelines when evaluating case-by-case proposals to transfer software documentation:

Purpose of the Transfer: Software documentation should be transferred for a specific purpose. Normally, the purpose will be to provide the recipient with the means to support end-items purchased from the U.S. or to facilitate U.S. collaboration in international cooperative research, development, and acquisition programs. The extent to which software documentation is approved for transfer should be commensurate with its intended use.

Security Concerns: Software documentation may or may not be sensitive depending on the information contained therein. Prohibiting transfers of software documentation is not always an effective way to protect information because of the availability of modem software tools and information in the commercial sector. Furthermore, normal operation of a system over time may reveal much, if not all, of the information contained in software documentation. Object code released in conjunction with approved sales of U.S. systems is vulnerable to reverse engineering. Foreign access to U.S. software documentation could compromise critical DoD system and operational capabilities, or reveal vulnerabilities and intelligence data. In addition to the compromise of military technology, it is important to assess whether the release of software documentation will increase the vulnerability of U.S. and allied C^4I infrastructure and the extent of understanding of these vulnerabilities by the recipient state. The only sure way to prevent access to critical military technology is to deny transfer of the end-item or to purge sensitive capabilities.

Interoperability: Transfers of software documentation may be used to facilitate integration and interoperability with the equipment of armed forces of allied and friendly nations.

Availability: The U.S. DoD investment in software is moving towards the use of commercial off the shelf (COTS) products. Consideration should be given to the possibility that software products that are the same as or similar to those proposed for transfer may be available from both foreign and domestic commercial and government sources.

Proprietary Rights: Transfer of software documentation requires the approval of the holder of the proprietary rights to that software documentation. The proponent for the software documentation transfer will identify the holders of the propriety rights and, if the proponent is not the holder, verify that the rights to transfer software documentation to the recipient have been obtained.

Cooperative Opportunities: DoD will consider pursuing government-to-government agreements to ensure that the USG benefits from transfers of software documentation intended for inclusion in foreign acquisition programs when these programs have potential for satisfying USG military requirements.

Liability: The release of software documentation could permit alteration of the software that has undergone validation testing and may be under contractor warranty. Foreign access to software documentation may result in changes that invalidate associated system warranties. Liability issues may arise in connection with the use, either domestic or foreign, authorized or unauthorized, of software documentation. These issues must be resolved before transfers occur when the USG is a party to the transfer.

DEFINITIONS:

Software: Programs, data bases, and associated documentation available on human and/or machine readable media such as paper, magnetic tapes, disks, or embedded firmware that operate computers.

Software documentation: Information in human-readable form, including computer source code listings and printouts which: documents the design or details of the computer software; explains the capabilities of the software; or provides operating instructions for using the software to obtain the desired results from a computer.

Source Code: Source code, a *subset* of computer software documentation, is a set of symbolic computer instructions that is written in a high-level/human-readable language that cannot be directly executed by the computer without first being translated into object code.

Object Code: The machine readable code.

Firmware: Implementation of software in hardware circuitry or read only memory.

Software Support: Resources such as people, facilities, documentation, information, and instrumentation to operate, maintain, or produce software products.

REVIEW OF THE GUIDELINES: These guidelines will be reviewed every two years at a minimum. More frequent reviews should be undertaken if technological or security circumstances dictate.