CHAPTER 4

CONTROLLED UNCLASSIFIED INFORMATION AND FOREIGN GOVERNMENT INFORMATION

A. INTRODUCTION

This chapter deals with two different types of information. The first is U.S. controlled unclassified information (CUI). The Arms Export Control Act (AECA) *(reference b)*, the Export Administration Act (EAA) (*reference e*), the Freedom of Information Act (FOIA) *(reference g)*, and Public Law (PL) 98-94 (1983) *(reference k)* are the primary statutes that provide the legal basis for the control of CUI covered by this handbook. The second is foreign government information, both classified and unclassified. The legal basis for protecting foreign government classified information and unclassified information provided in confidence is E.O. 12958, as amended *(reference i)*, which is implemented by 32 CFR Part 2001, Classified National Security Information Directive Number 1, and also referred to as the Information Security Oversight Office Directive 1 (or ISOO Directive No. 1). It is implemented in the Department of Defense (DoD) by DoD 5200.1-R *(reference j)*. This chapter will discuss policies and procedures for handling both types of information.

B. CONTROLLED UNCLASSIFIED INFORMATION

1. The term "Controlled unclassified information “or” CUI" is a term used in the DoD to collectively describe unclassified information to which access or distribution controls have been applied pursuant to the laws and regulations of the originating country. It is the presence of the access and/or distribution control markings that identify the information as “controlled unclassified information." In the United States, CUI is unclassified information that qualifies for exemption from mandatory disclosure under the FOIA, whether generated by DoD or another agency. In its simplest form, official U.S. Government information can be considered "controlled information;" it belongs to the U.S. Government. Just as the improper use of a company's proprietary information may damage the company that originated it, so too could the improper use of certain categories of government information likely cause damage to the government or its employees. DoD usually marks such information “For Official Use Only” but other markings are also used (e.g., Unclassified Controlled Nuclear Information (UCNI) and privacy statements). Other U.S. Government agencies apply different markings. The Department of Defense has several policies covering the disclosure of official information. DoD Directive 5400.4 *(reference ss)* governs testimony, prepared statements and other material provided to congressional committees the U.S. Congress might publish. DoD Directive 5405.2 *(reference tt)*

contains policy concerning release of official information in judicial proceedings. DoD Directive 5230.9 *(reference uu)* contains policies and procedures for the release of information for publication or public release. DoD Instruction 3200.14 (*reference vv*) and DoD Directives 5230.24 *(reference m)*, and 5230.25 *(reference l)* govern the release of DoD technical information. DoD 5400.7-R *(reference h)* contains the Department of Defense policies and procedures governing FOIA requests. Official information that meets the standards for security classification is classified and protected in compliance with E.O. 12958, Classified National Security Information Directive Number 1 (32 CFR Part 2001) (*reference n*), and DoD 5200.1-R (*reference j*).

2. The U.S. Congress has stated the U.S. public generally has the right to know what its government is doing. Therefore, the FOIA requires that government information be made available to the public, unless the information falls within one or more of nine exemption categories described in the Act and the appropriate U.S. Government official determines it should be withheld from disclosure. The first exemption category is classified information. The FOIA permits the withholding of any information properly and lawfully classified under the provisions of E.O. 12958. The other eight exemption categories deal with unclassified information.

a. Exemption two permits the withholding of information that pertains solely to the internal rules and practices of a government agency. This exemption has a high and low profile. The high profile permits the withholding of a document which, if released, would allow circumvention of an agency rule, policy, or statute, thereby impeding the agency in the conduct of its mission. The low profile permits withholding if there is no public interest in the document, and it would be an administrative burden to process the request;

b. Exemption three permits the withholding of information that a statute specifically exempts from disclosure by terms that permit no discretion on the issue, or in accordance with criteria established by that statute for withholding or referring to particular types of matters to be withheld;

c. The fourth exemption permits withholding information such as trade secrets and commercial and financial information obtained from a company on a privileged or confidential basis which, if released, would result in competitive harm to the company;

d. The fifth category exempts inter- and intra-agency memoranda that are deliberative in nature. This exemption is appropriate for internal documents that are part of the decision making process and contain subjective evaluations, opinions and recommendations;

e. Exemption six provides for the withholding of information, the release of which could reasonably be expected to constitute a clearly unwarranted invasion of personal privacy of individuals;

f. The seventh exemption permits withholding records or information compiled for law enforcement purposes that could reasonably be expected to interfere with law enforcement proceedings; would deprive a person of the right to a fair trial or impartial adjudication; could

reasonably be expected to constitute an unwarranted invasion of personal privacy of others; disclose the identity of a confidential source; disclose investigative techniques; or could reasonably be expected to endanger the life or physical safety of any individual;

g. The eighth exemption permits withholding records or information contained in or relating to examination, operation or condition reports prepared by, on behalf of, or for the use of any agency responsible for the regulation or supervision of financial institutions; and

h. The ninth exemption permits withholding records or information containing geological and geophysical information and data (including maps) concerning wells.

3. It is exemption category three of the FOIA, comprising information exempt from public disclosure pursuant to a statute, which is pertinent to the discussion of CUI involved the programs covered by this Handbook. A list of the most common statutes that fall within this exemption is at Appendix C. There are a number of other statutes and Appendix C provides guidance on locating these other statutes.

4. Within the list of statutes referred to above, it is PL 98-94 (*reference k*) that is of primary interest in the context of the export or disclosure of unclassified information in international defense programs.

a. It has been DoD policy for many years to place distribution statements on documents produced by or for DoD when the documents contained unclassified scientific and technical information. Until recent times, however, this policy was only marginally directed toward restricting the disclosure of such information to the public, and thus to foreign persons. Unfortunately, the practice did not always conform to the policy in many cases. The result was that sensitive scientific and technical information occasionally found its way into the public domain, including the foreign public.

b. This situation was compounded with the enactment of the FOIA. The FOIA made no provision for exempting unclassified government scientific and technical information from public disclosure, even for information that would be subject to export controls. Although the precise effect of this circumstance on the flow of sensitive U.S. technology overseas is debatable, there can be little doubt that unintended transfers of technology to foreign recipients occurred in this manner.

c. The situation was remedied in 1984. Enactment of P.L. 98-94 gave the Secretary of Defense authority to withhold from the public critical technologies.

d. To implement PL 98-94, the Department of Defense published DoD Directive 5230.25 (*reference l*) and updated the existing DoD Directive 5230.24 (*reference m*). The former interprets and amplifies the provisions of the law and establishes procedures both for withholding such information from the public and for allowing dissemination to those persons, inside and outside the U.S. Government, who have a demonstrable need for the information. The latter is a revision and update of the old DoD policy pertaining to the application of distribution statements to unclassified technical documents. A general

familiarity with the salient policy and procedural features of these two directives is essential to an overall understanding of the DoD policy governing the control of critical technology.

5. **DoD Directive 5230.25, "Withholding of Unclassified Technical Data from Public Disclosure"**

a. DoD Directive 5230.25 (*reference l*) applies to all unclassified technical data with military or space application in the possession of, or under the control of, a DoD component which may not be exported lawfully without approval, authorization or license under the EAA *(reference e)* or the AECA (*reference b*).

b. Critical technology consists of:

(1) Arrays of design and manufacturing know-how (including technical data);

(2) Keystone manufacturing, inspection and test equipment;

(3) Keystone materials; and

(4) Goods accompanied by sophisticated operation, application or maintenance know-how that would make a significant contribution to the military potential of any country or combination of countries and that may prove detrimental to the security of the United States (also referred to as militarily critical technology).

c. Technical data with military or space application are any blueprints, drawings, plans, instructions, computer software and documentation, or other technical information that can be used or be adapted for use to design, engineer, produce, manufacture, operate, repair, overhaul, or reproduce any military or space equipment or technology concerning such equipment.

d. DoD Directive 5230.25 does not govern the release of technical data by DoD Components to foreign governments, international organizations or foreign contractors that are carried out under a U.S. Government international program or a U.S. Government approved export authorization. As discussed in Chapter 2, an export authorization is required for commercial exports of this technical data unless it qualifies for an exemption under the ITAR *(reference c)* or the Export Administration Regulations (EAR) *(reference u)*. For commercial exports under the EAR and ITAR, the export authorization should contain the access, use and distribution restrictions that apply to critical technology approved for export to foreign governments or their contractors. A Form DSP-83, Nontransfer and Use Certificate, may also be required for the export of classified articles and technical data under the ITAR. For Government programs, the requirements should be included in the sales contract or agreement. (See also Chapter 2, Subsection C.1.a.)

e. DoD Directive 5230.25 requires that U.S. contractors be certified with the Defense Logistics Agency (DLA) to obtain technical documents containing critical technology from DoD sources. Since Canadian industry is by law a part of the North American Defense

Mobilization Base, they are also eligible for certification and access to most of this information on the same basis as U.S. registered contractors. (See subsection 8. below.)

6. **DoD Directive 5230.24, "Distribution Statements on Technical Documents"**

a. DoD Directive 5230.24 (*reference m*) requires all DoD Components that generate or are responsible for technical documents determine their distribution availability and mark them appropriately before primary distribution. Managers of technical programs are required to assign appropriate distribution statements to technical documents generated within their programs to control the secondary distribution of those documents. Therefore, technical data with military or space application also must be marked with a prescribed export warning statement, in addition to other markings authorizing or restricting secondary distribution.

b. The importance of applying this export warning statement is illustrated by the following:

(1) Regardless of any other distribution statements on the document, the export warning statement is the only one which has the legal basis (the AECA (*reference b*) or EAA (*reference e*) to support an exemption to the FOIA for unclassified technical information.

(2) This is the only statement which puts all holders on clear notice that transfer of such unclassified technical information to foreign recipients without proper U.S. Government authorization is a violation of law.

c. In addition to an export warning statement, or even if one is not applicable, all documents produced by or for the Department of Defense must be marked with a prescribed statement governing distribution if they fall within any of the following categories:

(1) Research, development, test or evaluation (RDT&E).

(2) Engineering, production or logistics.

(3) Operation, use or maintenance.

d. These distribution statements range from "approved for public release; distribution is unlimited" to "further dissemination only as directed by the controlling DoD office or higher DoD authority." Appendix D contains the export warning statements and a list of required distribution statements for unclassified technical documents, with supporting rationale for choosing the appropriate one.

7. **FOR OFFICIAL USE ONLY (FOIA) Marking.** If unclassified information is determined upon review to qualify for an exemption under FOIA exemption categories two through nine, the Department of Defense policy is to mark the data FOR OFFICIAL USE ONLY (FOUO), in addition to any other required distribution or control markings described in DoD Directive 5230.24 (reference m) or other applicable regulations.

a. DoD policy requires that the FOUO marking be applied when otherwise exempt information is generated. However, all official information must be reviewed before release to the public, including foreign governments and international organizations and their representatives. The release of the information to foreign nationals requires the consent of the originator.

b. FOUO information must be controlled in a manner sufficient to ensure that unauthorized persons do not gain access. Normally it is sufficient to lock the information in a desk drawer, bookcase, filing cabinet or similar container or a locked room to which only authorized persons have access. A FOUO cover sheet should be used to conceal the information when it is not in use and not secured. It may be sent via first-class mail or parcel post. It may be destroyed in any manner that would reasonably preclude easy reconstruction of the contents. Appropriate administrative disciplinary action shall be taken against those responsible for unauthorized disclosure. Unauthorized disclosure of FOUO that is protected by the Privacy Act (5 U.S.C. 552A, *(reference ww)*) may result in civil or criminal sanctions. See DoD 5400.7-R *(reference h)*. Unauthorized disclosures of technical data controlled by the AECA can result in criminal prosecution.

c. The processing and transmission of CUI by electronic means must be accomplished in a manner that ensures the confidentiality of the information. Web sites containing the CUI shall not be accessible to the general public. Therefore, heads of DoD components shall ensure that any DoD unclassified information which is placed on publicly accessible web sites (including the so-called ".mil" sites) has been reviewed and approved for public disclosure in compliance with DoD Directive 5230.9 (*reference uu*). Access to DoD information systems containing CUI (and classified information) shall be on a demonstrated need-to-know basis and in compliance with DoD Directive 8500.1 (*reference* xx), DoD 5200.1-R (*reference j*), and the DoD Web Site Administration Policies and Procedures. The latter publication is available at http://www.defenselink.mil/webmasters/policy/dod_web_policy_12071998_with_amend. Access to the information system by foreign nationals (including liaison officers, exchange officers, and cooperative program personnel) and contractors, as well as connectivity to allied systems, shall be controlled in compliance with DoD Directive 8500.1 (reference xx) and the National Industrial Security Program Operating Manual (NISPOM) (*reference y*). Decisions on access by representatives of foreign governments and international organizations (such as liaison officers, exchange officers, and cooperative program personnel) shall be made in foreign disclosure channels by Principal or Designated Disclosure Authorities; they may have access to only that information that can be disclosed to their government. A DoD web site shall not process CUI or any official DoD information that has not been cleared for public release unless the site employs adequate security and access controls. The minimum DoD information system access requirement shall be a properly administered and protected by individual identifier and password. When CUI is to be discussed or transmitted via fax, secure voice and facsimile systems should be used.

8. **U.S.-Canada Joint Certification Program.** The Joint Certification Program (JCP) benefits both U.S. and Canadian defense and high technology industries by facilitating their access to unclassified critical technology in the possession or under the control of the U.S. Department of

Defense or the Canadian Department of National Defence (DND). Certification under the JCP establishes the eligibility of a U.S. or Canadian contractor to receive technical data governed, in the United States, by DoD Directive 5230.25 (*reference l*) and, in Canada, by the Technical Data Control Regulations (TDCR) *(reference yy)*. The U.S./Canada Joint Certification Program is part of the Defense Logistics Information Service (DLIS), Battle Creek, Michigan.

a. As a condition of receiving DoD- or DND-controlled technical data, the contractor agrees to use the data only in ways mandated by DoD Directive 5230.25 or the TDCR. The contractor must certify that it needs the technical data to bid or perform on a contract with an agency of the U.S. or Canadian Government, as applicable, or for other legitimate business purposes. Other legitimate business purposes include:

(1) Providing or seeking to provide equipment or technology to a foreign government with the prior approval of the U.S. or Canadian Government, as applicable;

(2) Bidding or preparing to bid on a sale of surplus property;

(3) Selling or producing products for the U.S. or Canadian commercial domestic marketplace, or for the commercial foreign market place, providing that any required export license is obtained from the appropriate U.S. or Canadian licensing authority;

(4) Engaging in scientific research in a professional capacity for either of the two defense establishments; or

(5) Acting as a subcontractor for a concern described in (1) through (4).

b. The contractor also:[1]

(1) Certifies that the person who will receive the data on behalf of the contractor is a U.S. citizen or person lawfully admitted into the United States for permanent residence and is located in the United States.

(2) Acknowledges its responsibilities under U.S. export control laws and regulations and agrees that it will not disseminate any export-controlled technical data subject to this Directive in violation of such laws and regulations.

(3) Agrees that it will not provide unauthorized access to export-controlled technical data subject to DoD Directive 5230.25 (*reference l*) to persons other than its employees or persons acting on its behalf.

(4) Certifies to the best of its knowledge and belief that no person employed by it, or acting on its behalf, who will have access to the technical data, who is debarred, suspended, or otherwise ineligible from performing on U.S. Government contracts; or has violated U.S. export control laws or previous certifications under DoD Directive 5230.25.

[1] Canadian contractors may qualify by submitting an equivalent certification.

(5) Certifies it is not debarred, suspended, or otherwise determined ineligible by the U.S. Government to perform on U.S. Government contracts, has not been convicted of violations of export control laws and has not been disqualified under the provisions of DoD Directive 5230.25.

c. The Department of Defense also exempts certified Canadian contractors from the need to obtain approval from DoD for unclassified visits to DoD contractor installations to obtain unclassified militarily critical technical data. Canada's Industrial Security Program procedures also allow for direct contractor-to-contractor arrangements for such visits by U.S. certified contractors. As a result, JCO certified U.S. and Canadian contractors can make visit arrangements involving only unclassified technical data directly with a U.S. or Canadian contractor.

d. This program does not extend to company proprietary technical data that is not controlled by DoD or DND. Therefore, it does not govern the private exchange of industry-generated export-controlled technical data. In these cases contractors must follow the guidelines established in U.S. or Canadian export control regulations, as applicable.

e. The U.S.-Canada Joint Certification Program pamphlet *(reference zz)* contains additional information, procedures and restrictions. This pamphlet is available from:

U.S./Canada Joint Certification Program
Defense Logistics Information Service (DLIS)
74 Washington Avenue North Ste.7
Battle Creek, Michigan 49017-3084
jcp-admin@dlis.dla.mil

C. FOREIGN GOVERNMENT INFORMATION

1. Policy

a. Foreign government information (FGI) is defined by Executive Order 12958, as amended, (*reference i*) as:

(1) Information provided to the United States by a foreign government or governments, an international organization of governments or any element thereof, with the expectation that the information, the source of the information, or both, are to be held in confidence;

(2) Information produced by the United States pursuant to or as a result of a joint agreement with a foreign government or governments, or an international organization of governments or any elements thereof, requiring that the information, the arrangement, or both, are to be held in confidence; or

(3) Information received and treated as "Foreign Government Information" under the terms of a predecessor order.

b. FGI must retain its original classification, or be assigned a U.S. classification designation that will provide protection equivalent to that provided by the furnishing government or organization.

c. E.O. 12958, as amended, states that foreign government information is in a category of information that is classifiable. Therefore, foreign government unclassified information that is provided in confidence may be classified and marked "Confidential--Modified Handling Authorized." When so marked, it shall be safeguarded in accordance with Classified National Security Information Directive No. 1, (32 CFR 2001), reference n., and DoD 5200.1-R. If there is uncertainty concerning whether the information is to be handled "in confidence", the providing government or international organization should be consulted.

d. When unclassified foreign government "in confidence" information is involved in an international program, program documentation (e.g., the MOU, PSI, or contract) should include procedures on handling the information.

2. **Procedures.**

a. Foreign government designations for classified information generally parallel U.S. security classification designations. However, some foreign governments have a fourth level of classification, RESTRICTED, and a category of unclassified that is protected by law and is provided on the condition that it is treated "in confidence." This information must be classified under E.O. 12958 in order for it to be provided the degree of protection required by the originator. Foreign government RESTRICTED information and unclassified information provided "in confidence" shall be marked to identify the originating government and whether it is RESTRICTED or provided "in confidence." Additionally, to ensure protection under E.O. 12958, such information will be marked "CONFIDENTIAL--Modified Handling Authorized." This U.S. marking should be removed, however, prior to returning such information to the originating government. This information may be safeguarded in a manner that is similar to that for "FOR OFFICIAL USE ONLY." Classified FGI and unclassified FGI provided in confidence must be transferred through official government-to-government channels, or other channels agreed upon in writing by the governments. Foreign government classification designations and U.S. equivalents are at Appendix E. (Note: See subparagraph j, below, for United Kingdom (UK) exception.)

b. U.S. documents containing FGI must be marked with a notation that states "THIS DOCUMENT CONTAINS (indicate country of origin) INFORMATION." In addition, the portions containing FGI must be marked to identify the classification level and country of origin (e.g., UK--C or UK--R). The foreign government document or authority, on which the classification is based, in addition to the identification of any U.S. classification authority, must be identified on the "Derived From" line. A continuation sheet should be used for multiple sources, if necessary. A U.S. document marked as described herein cannot be

downgraded below the highest level of FGI contained in the document or be declassified without the written permission of the foreign government or international organization that originated the information.

c. Security clearances issued by the U.S. Government are valid for access to classified FGI of a comparable level.

d. FGI or material classified TOP SECRET, SECRET, or CONFIDENTIAL must be stored in the manner required for U.S. information of the same level by DoD 5200.1-R (*reference j*) and the NISPOM *(reference y)*. To avoid inadvertent compromise, foreign government classified material must be stored in a manner that will avoid commingling with other material. For small volumes of material, separate files in the same vault, container, or drawer will suffice. FGI marked "CONFIDENTIAL-Modified Handling Authorized" may be stored in a locked desk, cabinet or similar locked container, or in a locked room to which access is controlled.

e. Persons having access to FGI must be notified of their responsibilities for handling the information. Records will be maintained for FGI as follows:

(1) TOP SECRET--records shall be maintained of the receipt, annual inventory, internal distribution, external dispatch, destruction, annual inventory, access, reproduction, and transmittal. Reproduction requires the consent of the originator. Destruction shall be witnessed. Records shall be maintained for five years.

(2) SECRET--records shall be maintained of the receipt, distribution, external dispatch, and destruction. Other records may be required by the originating government. It may be reproduced to maintain mission needs, but reproduced copies shall be accounted for and recorded. Records shall be maintained for three years.

(3) CONFIDENTIAL--records shall be maintained of the receipt and external dispatch. Other records may be required by the originating government. Records shall be maintained for two years.

(4) CONFIDENTIAL-Modified Handling Authorized--records are not necessary unless required by the originating government.

f. FGI can not be disclosed to nationals of third countries, including foreign nationals who are protected individuals (resident aliens), or to any other third party, or used for other than the purpose for which the foreign government provided it without the originating government's written consent. Government agencies must submit requests for other uses or further disclosure to the originating government. Contractors will submit their requests through the contracting U.S. Government agency for U.S. contracts and the Defense Security Service for direct commercial contracts.

g. The ITAR requires a license for the commercial export or re-export of FGI unless the information is exported, in its original form, to the original source of import.

h. The transmission of FGI within the United States among U.S. Government agencies and U.S. contractors and between U.S. contractors with a need-to-know must be in accordance with DoD 5200.1-R (*reference j*) and the NISPOM (*reference y*).

i. The international transfer of foreign government classified information must be through a government-to-government transfer in compliance with Chapter 6 of this handbook.

j. On January 27, 2003, the DoD and the UK Ministry of Defence (MOD signed a "Security Implementing Arrangement," which replaces the US/UK industrial security agreement. Among other things, the new arrangement removes U.S. Government security oversight responsibility for UK Restricted information that is provided to a U.S. defense contractor. It is now the responsibility of the UK or U.S. contracting activity to incorporate requirements in contracts for the protection of the UK Restricted information. As the result of this new arrangement, the following additional changes are effective April 2003:

(1) The requirements of the National Industrial Security Operating Program Manual (NISPOM) no longer apply to UK Restricted information;

(2) The information is no longer the oversight responsibility of the Defense Security Service (DSS);

(3) A contractor's obligation to protect the information will be included in the applicable contract;

(4) A personnel and facility security clearance are not necessary for access;

(5) The information may be transmitted directly to a U.S. contractor by a UK contractor or the UK MOD;

(6) UK Restricted documents may be single wrapped and transmitted by First Class Mail within the United States; transmissions outside the United States will be double wrapped with the inner wrapper marked "UK Restricted." International transfers shall be by one of the means authorized for U.S. classified information, by international airmail, or by express commercial courier services (government-to-government transfers are not required);

(7) The information may be transmitted or accessed electronically via a public network (like the internet) using government or commercial encryption devices approved by the Ministry of Defence (MOD). Telephone conversations, videoconferencing or facsimile transmissions within the United States may be conducted without encryption. International transmissions by the foregoing means may be conducted without encryption, if encryption is not available.

(8) Guidance regarding the use of communications and information systems for storing, processing, and transmitting UK Restricted information will be

incorporated into the applicable contract Restricted Conditions Requirements Clause; contractors may self-certify and accredit information systems using guidance provided in the contract clauses;

(9) Unless prohibited in the UK contract, U.S. contractors may sub-contract to contractors in the United States or in the United Kingdom without prior approval of the UK MOD; the contract Restricted Conditions Requirements Clause will be included in any sub-contract; sub-contracts to be awarded outside the United States or the United Kingdom require the approval of the UK MOD;

(10) When the U.S. DoD Component provides UK Restricted information to either U.S. or UK contractors, the Component will provide safeguarding guidance;

(11) An export license for UK Restricted will be processed in the same manner as an unclassified export; government-to-government transfer is not required, and

(12) Visits to UK MOD facilities and to contractor facilities in the United States or in the United Kingdom where access to only unclassified or UK Restricted information do not require a government approved visit authorization. However, it is the responsibility of the U.S. contractor facility that is hosting the visit to ensure that all export control and foreign disclosure requirements are satisfied prior to the disclosure of controlled information.