

27 JULY 1994



Scientific/Research and Development

**DISSEMINATING SCIENTIFIC AND
TECHNICAL INFORMATION**

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the SAF/AAD WWW site at: <http://afpubs.hq.af.mil>. If you lack access, contact your Publishing Distribution Office (PDO).

OPR: SAF/AQT (Dr C. J. Chatlyne)
Supersedes AFR 80-34, 5 December 1985 and
AFR 83-3, 1 October 1990.

Certified by: SAF/AQT (Col A. Michael Higgins)
Pages: 21
Distribution: F

This instruction implements AFR 61-2, *Management of Scientific and Technical Information*; Department of Defense (DoD) Directive 5230.24, *Distribution Statements on Technical Documents*, 18 March 1987; and DoD Directive 5230.25, *Withholding Unclassified Technical Data from Public Disclosure*, 6 November 1984. It tells how to mark scientific, technical, engineering, production, and logistics data to show the extent to which personnel may disseminate the data. It describes the contractor certification process for access to unclassified, militarily-critical technical data and establishes procedures for withholding or disseminating such data. It applies to all technical publications and documents generated by all Air Force-funded research, development, test, and evaluation (RDT&E) programs, including working papers, memoranda, and preliminary reports, if those documents are not in the public domain, but are likely to be disseminated outside DoD. It also applies to engineering drawings, standards, specifications, technical manuals, blueprints, drawings, plans, instructions, computer software and documentation, photographs, technical orders, databases, and any information that can be used or adapted for use to design, engineer, produce, manufacture, operate, repair, overhaul, or reproduce any military or space equipment or technology concerning that equipment. It applies to any medium that transfers information, including paper, microform, electronic storage, and video recordings. It does not apply to cryptographic and communications security documents, communications and electronic intelligence, and other categories that the Director, National Security Agency, or the Chief, Central Intelligence Agency, designates. It does not apply to classified technical documents containing "restricted data" and "formerly restricted data" defined in the Atomic Energy Act of 1954, as amended. (See joint Department of Energy and DoD directives for distribution, control, and marking requirements.)

SUMMARY OF REVISIONS

This instruction updates, clarifies, and streamlines previous guidance.

1. Responsibilities:

1.1. All Air Force components that originate or are responsible for technical documents must determine the documents' distribution availability and mark them appropriately before disseminating the documents.

1.2. Commanders and directors of Air Force activities appoint local coordinators of export-controlled technical data.

1.3. The coordinator (usually the local scientific and technical information officer) coordinates release of export-controlled technical data to certified contractors.

1.4. Air Force personnel who originate or are responsible for technical documents:

- Mark documents with proper distribution statements before disseminating documents.
- Send requests for documents to established document repositories, such as the Defense Technical Information Center (DTIC).
- When documents are not at repositories, release documents only to requestors who have the appropriate need-to-know and are certified with the Defense Logistics Support Center (DLSC).
- Mail documents containing export-controlled data only to the document custodian listed in block 3 of DD Form 2345, **Militarily Critical Technical Data Agreement**. *Note: There is no requirement that the company official who certifies the form in block 6 must sign document requests.*
- When data packages contain export-controlled data, include with announcements for the data (for example, requests for proposal), explanations that requestors must be certified with Defense Logistics Support Center (DLSC) and include information on the certification process.

1.5. The public affairs office must review documents that originators recommended for public release in accordance with AFPD 35-1, *Public Affairs Management*.

2. Marking Technical Documents with Distribution-Limitation and Export-Control Statements:

2.1. Mark all technical documents that may be disseminated outside the DoD with one of the seven distribution statements listed in **Attachment 2**, and the following export control notice if the document contains export-controlled technical data. *Note: Distribution statements provide options ranging from unlimited distribution to no secondary distribution without specific approval of the originator.* Review the data categories before assigning a distribution statement, and use only the statements in **Attachment 2**. Fill in the reason, the date of determination, and the controlling DoD office.

WARNING--This document contains technical data whose export is restricted by the Arms Export Control Act (Title 22, U.S.C. 2571 et seq.) or Executive Order 12470. Violation of these export-control laws is subject to severe criminal penalties. Dissemination of this document is controlled under DoD Directive 5230.25 and AFI 61-204.

2.2. When providing technical documents to personnel from another DoD activity, mark documents to minimize the chance that DoD personnel might inadvertently give documents to inappropriate recipients.

2.3. Mark unclassified limited documents (i.e. documents not approved for public release) and classified documents with the following:

DESTRUCTION NOTICE--For classified documents, follow the procedures in DoD 5220. 22-M, *Industrial Security Manual*, section 11-19, or DoD 5200.1-R, *Information Security Program Regulation*, chapter IX. For unclassified, limited documents, destroy by any method that will prevent disclosure of contents or reconstruction of the document.

2.4. You do not have to put a distribution statement on contractor-technical proposals or documents submitted in anticipation of award of contracts. Follow the guidelines in paragraphs 2.5.3 and 6.3 when working with contractor technical proposals that contain contractor limited rights data.

2.5. Guidance on release of software is in AFI 33-114, *Command, Control, Communications, and Computer (C4) Software Management*. **Note: Only the software developer or office of primary responsibility may release source code; secondary distribution is limited to the application software (the object code).**

2.6. The following is specific guidance for assigning distribution statements:

2.6.1. Distribution statements A-X may be applied to unclassified Air Force technical documents, while only distribution statements B-F may be applied to classified documents.

2.6.2. When a classified document is declassified, retain the original distribution statement until the controlling office either removes or changes the statement. When a classified document is declassified and has no distribution statement, handle the document as distribution F until the controlling office assigns a distribution statement.

2.6.3. Mark and control scientific and technical documents that include contractor-imposed limited-rights legends and computer software that includes contractor-imposed restricted-rights legends according to subpart 27.4 of the Defense Federal Acquisition Regulation Supplement.

2.6.4. Do not disseminate technical documents in draft or preliminary form without assigning distribution statements.

2.7. Distribution statements remain in effect until the controlling DoD office changes or removes them. Each controlling DoD office must establish a procedure for reviewing its documents periodically or when they receive a request for the document for possible changes or removal of distribution statements. For unclassified documents, the controlling DoD office must obtain public release determination according to AFPD 35-1 before assigning distribution statement A.

2.8. Controlling DoD offices must notify DTIC and other concerned document-dissemination activities when:

- Program management responsibility is transferred, addresses of designated controlling DoD offices are changed, or controlling DoD offices are redesignated.
- Classification markings, distribution statements, or export control statements are changed or removed.

2.9. For technical publications, place the distribution statement on the front cover, title page, and SF 298, **Report Documentation Page**. If the technical document is not intended for publication and

does not have a cover or title page, stamp, print, or write the distribution statement on the front page of the document.

2.10. When possible, put the portions of the document that contain information requiring distribution limitation in an appendix or separate volume to permit broader distribution of the basic document. Write the abstract on the SF 298 so that the information in the abstract will not have a limited distribution (i.e. that it is approved for public release).

2.11. You must include distribution statements and export-control notices on newly created documents.

2.11.1. You do not need to apply markings to technical documents that were created before the implementation of this instruction until someone asks for them. Mark and control them properly before disseminating them.

2.11.2. When older documents contain superseded distribution statements, convert the statements as follows:

2.11.2.1. Assign distribution statements C, B, E, and F to technical documents bearing distribution statements 2, 3, 4, and 5 of superseded DoD Directive 5200.20, *Distribution Statements (Other than Security) on Technical Documents*, 29 March 1965, respectively.

2.11.2.2. Do not reevaluate technical documents with distribution statements A and B of cancelled DoD Directive 5200.20, *Distribution Statements on Technical Documents*, 24 September 1970 or documents with distribution statements A-F contained in Secretary of Defense Memorandum "Control of Unclassified Technology with Military Applications," 18 October 1983.

3. Confirming the Certification of US Contractors:

3.1. In order to receive export-controlled technical data contractors must be certified by the DLSC. Air Force activities may confirm a firm's status by reviewing the certified contractor access list (CCAL), which DLSC maintains on an electronic bulletin board system accessible on a personal computer by modem or the Defense Data Network (DDN). Call DLSC at 1-800-352-3572 for information on how to access the CCAL. (Certification process is described in **Attachment 3**.)

3.2. When you receive a request for export-controlled technical data from someone who is not certified, tell the requestor in writing why his or her request was denied. See **Attachment 4** for a sample letter, which you may tailor to fit local needs. Include a copy of the information sheet on the certified contractor program (**Attachment 5**).

4. Handling Certified Contractor Requests for Export-Controlled Technical Data:

4.1. A controlling Air Force activity, or a repository responsible for secondary distribution of technical data, may release export-controlled technical data to a currently certified US contractor, unless:

4.1.1. The requested information is not related to the contractor's certification.

- Use the sample letter of denial at **Attachment 6**, example 1 (tailored for local needs) to tell the requestor why his or her request is denied.
- Tell the requester that he or she can provide additional information or apply to DLSC for certification in that area.

4.1.2. The firm will not be using the information to bid or perform on an Air Force or other Government agency contract and release of the information might jeopardize US technical or operational military advantages.

- Use the sample letter of denial at **Attachment 6**, example 2 (tailored for local needs) to tell the requestor why his or her request is denied. Coordinate the letter with the legal office.
- Tell the requester that he or she can appeal the decision.

4.1.3. The validity of the contractor's qualifications is in doubt. Coordinate with the legal office or with DLSC.

4.1.4. The requestor is a debarred contractor.

NOTE:

Cite 10 U.S.C. 130 as implemented by DoD Directive 5230.25 and this instruction when denying requests for export-controlled technical data.

4.2. An Air Force activity sends requests from foreign governments to its foreign disclosure office (FDO). If the foreign government is not bidding on or supporting an Air Force or other Government contract, tell the contractor to submit the request through its embassy. The embassy may submit the request to the Deputy Undersecretary of the Air Force for International Affairs (SAF/IA), Country Director. (See AFPD 16-2, *Foreign Disclosure of Classified and Unclassified Military Information to Foreign Governments and International Organizations*, and AFI 16-201, *Foreign Disclosure of Classified and Unclassified Military Information to Foreign Governments and International Organizations*.)

5. Handling Freedom of Information Act (FOIA) Requests for Export-Controlled Technical Data.

Follow the instructions in AFI 37-131, *Air Force Freedom of Information Act Program*, when you get a request for export-controlled, technical data under FOIA from someone other than a certified US contractor.

- Use the third exemption of 5 U.S.C. 552(b)(3) to deny those requests.
- Use the sample letter of denial at **Attachment 7** (tailored for local needs) to tell the requestor why his or her request is denied.
- Tell the requester that he or she can appeal the decision.
- Follow the instructions in AFI 37-131 when someone appeals your decision.
- Direct FOIA requests from the public to the FOIA manager.

NOTE:

Process FOIA requests for export-controlled technical data from a certified US contractor according to section 4 of this instruction and inform the requestor of this action.

6. Sending Technical Data to Certified Contractors:

6.1. You may charge for copying, certifying, and searching records. (See AFPAM 37-145, *Schedule for Fees for Copying, Certifying, and Searching Records and Other Material*.) Tell people asking for

information in the Defense Technical Information Center (DTIC) collection to contact DTIC for the data.

6.2. Do not release documents marked with distribution statement F without getting the originator's approval first. Tell the requestor that you are asking for authority to release the data. The controlling activity must ensure the requestor is a current, certified, US contractor before approving release of the information.

6.3. Coordinate with the legal office that services the contracting activity that issued the contract before releasing proprietary material.

6.4. Include the notice at **Attachment 8** with any release of export-controlled technical data. Use one copy of the notice regardless of the number of documents included in the release.

7. Secondary Dissemination of Export-Controlled Technical Data:

7.1. Certified contractors do not need Air Force permission to disseminate export controlled technical data when it is used for purposes consistent with the certification unless the Air Force has told them that they can't. The contractor must include a copy of the export-control notice (**Attachment 8**). They may disseminate the data:

- To any foreign recipient approved, authorized, or licensed under Executive Order 12470 or the Arms Export Control Act.
- To another currently certified US contractor when that contractor is using the information under the guidelines in this AFI.
- To the Departments of State and Commerce so that the company can apply for approvals, authorizations, or licenses for export under the Arms Export Control Act or Executive Order 12470.
- To Congress or any Federal, state, or local governmental agency so the company can meet regulatory, legal, or court-order requirements.

7.2. A certified US contractor must get the controlling Air Force activity's permission before disseminating export-controlled technical data not specifically authorized by this instruction. Give contractors a written statement giving them permission or telling them why they may not disseminate the data. The statement must be delivered within 45 days of the denial and must tell them that they may appeal the decision to the major command (MAJCOM) scientific and technical information (STINFO) officer.

NOTE:

Unauthorized redissemination of export-controlled technical data can occur by publishing articles in open literature, in advertising or in promotional materials, in conducting educational and training courses, and by similar means whereby persons or entities not authorized by this instruction to have access can obtain access to the data.

8. Dealing with Violations of US Export Control Law:

8.1. Air Force activities must report to their MAJCOM STINFO Officer when a certified US contractor:

- Violates US export control law.

- Makes certifications in bad faith.
- Omits or misstates material facts.

8.2. Report violations involving a foreign contractor or other representative of a foreign nation to the MAJCOM STINFO officer, the FDO (in accordance with AFI 16-201 and to the Air Force Office of Special Investigations).

8.3. After coordinating with the MAJCOM staff judge advocate (SJA), the MAJCOM STINFO officer temporarily revokes the contractor's qualification. (*Note: If further legal coordination is required, the MAJCOM SJA coordinates with the Air Force Office of the Judge Advocate General and the Office of the General Counsel of the Air Force.*)

8.3.1. The STINFO officer:

- Immediately notifies the contractor and DLSC that the contractor's certification has been revoked.
- Gives the contractor an opportunity to respond in writing to the information on which the temporary revocation is based.

8.3.2. Based on the contractor response, the STINFO officer does one of the following:

- Reinstates the contractor when he or she presents sufficient information to show that the basis for the revocation was in error or has been remedied.
- Recommends DLSC disqualify the contractor when he or she does not provide enough information within 60 days to remove the revocation.

CLARK G. FIESTER
The Assistant Secretary of the Air Force
for Acquisition

Attachment 1

GLOSSARY OF REFERENCES, ABBREVIATIONS AND ACRONYMS, AND TERMS

References

DoD 5200.1-R, *Information Security Program Regulation*

DoD 5220.22-M, *Industrial Security Manual*

DoDD 5230.11, *Disclosure of Classified Military Information to Foreign Governments and International Organizations*

DoDD 5230.20, *Visits and Assignments of Foreign Representatives*

DoDD 5230.24, *Distribution Statements on Technical Documents*

DoDD 5230.25, *Withholding of Unclassified Technical Data feigdiic Dechl(o)0(n)re DiAF(e)PD 16-7(n)2*

MAJCOM—Major Command

OUSDRE—Office of the Under Secretary of Defense (Research and Engineering)

STINFO—Scientific and Technical Information

Terms

Certified Contractor—Private individual or enterprise located in the United States or Canada who is certified and registered with the Defense Logistics Service Center for access to export-controlled technical data.

Certified Contractor Access List (CCAL)—Listing of US contractors who are registered and certified to receive export-controlled technical information. The Defense Logistics Support Center (DLSC) maintains the CCAL on an electronic bulletin board system. Contact DLSC on DSN 369-6814 or toll-free commercial 1-800-352-3572 for information.

Controlling DoD Office—DoD activity that sponsored the work that generated the technical data or the office that receives the data on behalf of a Government agency and has the responsibility for distributing the data to eligible recipients.

Data Custodian—Person designated at a certified contractor facility to receive and disseminate controlled technical data.

Export Administration Act—Any of the laws that have been codified at 50 U.S.C. Appendix 2401-2420.

Export-Controlled Technical Data—Data that cannot be lawfully exported without the approval, authorization, or license under US export control laws. The controlling regulations and documents are the International Traffic in Arms Regulation (ITAR), the US munitions list, and the militarily critical technologies list (MCTL).

Export Administration Regulations (EAR)—Controls export of dual-use items (materials with both civilian and military uses) specified on the commodity control list. The EAR is administered by the Bureau of Export Administration, US Department of Commerce, and implements the Export Administration Act of 1979.

Intending US Citizen—An alien who falls into one of the following categories:

- Permanent residents
- Temporary residents (individuals who have gone through or are in the process of going through the amnesty legalization program)
- Individuals admitted as refugees
- Individuals granted asylum

International Traffic in Arms Regulation (ITAR)—Controls the export of defense articles specified in the US Munitions List and technical data directly related to them. ITAR is administered by the Office of Defense Trade Controls, US Department of State, and implements the US Arms Export Control Act. It has jurisdiction over:

- Information (including classified) relating to defense articles and defense services.
- Information covered by an invention secrecy order.

- Information directly related to designing, engineering, developing, producing, processing, manufacturing, using, operating, overhauling, repairing, maintaining, modifying, or reconstructing defense articles. It also includes information that advances the state-of-the-art of articles in the US Munitions List, including the technology used to procure or maintain these components. It does not include information concerning general scientific, mathematical, or engineering principles or theory.

Limited Document—Any document that is not approved for public release.

Militarily Critical Technologies List (MCTL)—The list issued by DoD under authority of the Export Administration Act. The MCTL lists technologies not possessed by countries to which the United States controls exports, and which, if exported, would permit a significant advance in a military system of any such country.

Militarily Critical Technology—Technologies that consist of:

- Arrays of design and manufacturing know-how (including technical data).
- Keystone manufacturing, inspection, and test equipment.
- Keystone materials.
- 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 security of the United States or Canada (also referred to as critical technology).

US Munitions List (22 CFR 121).— This list designates defense articles and defense services that are subject to ITAR, where:

- Defense articles are those items designated in the US Munitions List that must be export controlled, and includes models, mock-ups, and any other devices that reveal technical data related directly to those articles.
- Defense services means:
- Furnishing assistance, including training to foreign persons, in the design, engineering development, production, processing, manufacture, use, operation, overhaul, repair, maintenance, modification, or reconstruction of defense articles, whether in the United States or abroad.
- Furnishing any technical data to foreign persons, whether in the United States or abroad.

Attachment 2

DISTRIBUTION STATEMENTS AND THEIR CORRESPONDING REASONS FOR USE

DISTRIBUTION A. Approved for public release; distribution unlimited.
DISTRIBUTION B. Distribution authorized to US Government agencies only (reason) (date of determination). Other requests for this document shall be referred to (controlling DoD office).
DISTRIBUTION C. Distribution authorized to US Government agencies and their contractors (reason) (date of determination). Other requests for this document shall be referred to (controlling DoD office).
DISTRIBUTION D. Distribution authorized to DoD and US DoD contractors only (reason) (date of determination). Other requests for this document shall be referred to (controlling DoD office).
DISTRIBUTION E. Distribution authorized to DoD components only (reason) (date of determination). Other requests for this document shall be referred to (controlling DoD office).
DISTRIBUTION F. Further dissemination only as directed by (controlling office) (date of determination) or DoD higher authority.
DISTRIBUTION X. Distribution authorized to US Government agencies and private individuals or enterprises eligible to obtain export-controlled technical data in accordance with DoDD 5230.25 (date of determination). Controlling DoD office is (insert).

“REASON”	STATEMENT					
	B	C	D	E	F	X
ADMINISTRATIVE OR OPERATIONAL USE. To protect technical or operational data or information from automatic dissemination under the international exchange program or by other means. This protection covers publications required solely for official use or strictly for administrative or operational purposes. This statement may be applied to manuals, pamphlets, technical orders, technical reports, and other publications containing valuable technical or operational data.	X	X	X	X		
CONTRACTOR PERFORMANCE EVALUATION. To protect information in management reviews, records of contractor performance evaluation, or other advisory documents evaluating programs of contractors.	X			X		

CRITICAL TECHNOLOGY. To protect information and technical data that advance current technology or describe new technology in an area of significant or potentially significant military application or that relate to a specific military deficiency of a potential adversary. Information of this type may be classified. When unclassified, technology is export controlled.	X	X	X	X
DIRECT MILITARY SUPPORT. The document contains export-controlled technical data of such military significance that release for purposes other than direct support may jeopardize an important technological or operational US military advantage. Designation of such data is made by competent authority in accordance with DoDD 5230.25.				X
FOREIGN GOVERNMENT INFORMATION. To protect and limit distribution in accordance with the desires of the foreign government that furnished the technical information. Information of this type normally is classified at CONFIDENTIAL or higher in accordance with DoD 5200.1-R	X	X	X	X
PREMATURE DISSEMINATION. To protect patentable information on systems or processes in the developmental or concept stage from premature dissemination.	X			X
PROPRIETARY INFORMATION. To protect information not owned by the US Government and protected by a contractor's "limited rights" statement, or received with the understanding that it not be routinely transmitted outside the US Government.	X			X
SOFTWARE DOCUMENTATION. Releasable only in accordance with DoDI 7930.2.	X	X	X	X
TEST AND EVALUATION. To protect results of test and evaluation of commercial products or military hardware when such disclosure may cause unfair advantage or disadvantage to the manufacturer of the product.	X			X

<p>SPECIFIC AUTHORITY. To protect information not specifically included in the above reasons and discussions but which requires protection in accordance with valid documented authority such as Executive Orders, classification guidelines, DoD or DoD-component regulatory documents. When filling in the reason, cite "specific authority (identification of valid documented authority)."</p>	X	X	X	X	X	
--	---	---	---	---	---	--

Attachment 3

CONTRACTOR CERTIFICATION PROCESS FOR ACCESS TO EXPORT-CONTROLLED TECHNICAL DATA

Contractor Certification Process for Access to Export-Controlled Technical Data. To get certification, US and Canadian contractors submit a completed DD Form 2345, **Militarily Critical Technical Data Agreement**, to the US and Canadian Joint Certification Office (JCO). The JCO confirms the contractor's information, signs the form, and returns it to the contractor.

A3.1. Because DoD activities mail technical data to the location shown on the form, each corporate subsidiary or division requesting technical data must submit its own form to the JCO.

A3.2. Contractors designate a data custodian for the facility, either by name or by position. This person receives and disseminates controlled (militarily critical) technical data. *Note: The data custodian at a US contractor facility must be a US citizen or an intending US citizen.* The data custodian at a Canadian contractor facility must be a Canadian or US citizen or a person admitted lawfully for permanent residence into Canada.

A3.3. The contractor must agree to use the data to bid or perform on a contract with a US or Canadian agency or for other legitimate business purposes such as:

- Providing or seeking to provide equipment or technology to a foreign government. *Note: US or Canadian Government must approve sale or transfer before the contractor receives the information.*
- Bidding or preparing to bid on surplus Government property.
- Selling or producing products for the US or Canadian commercial domestic marketplace.
- Selling or producing products for the commercial foreign marketplace. *Note: The contractor must have an export license from the appropriate US or Canadian licensing authority.*
- Engaging in scientific research in a professional capacity for either the DoD or the Canadian Department of National Defense.
- Acting as a subcontractor for any of the above efforts.

A3.4. Contractors agree not to publicly disclose any controlled unclassified data, unless the controlling office authorizes it, and to limit access to their employees who meet the following citizenship requirements:

- US citizens or intending citizens if the facility is located in the United States.
- Canadian or US Citizens or persons admitted lawfully for permanent residence in Canada if the facility is located in Canada.

A3.5. Certified contractors may:

- Ask for controlled unclassified technical data.
- Respond to defense-related solicitations and enter into defense-related contracts that include a requirement for controlled unclassified technical data.

- Attend restricted gatherings where controlled unclassified technical data are presented (for example: symposia, conferences, meetings that publicize advance requirements, pre-bid, pre-solicitation, and pre-award conferences).
- Visit and exchange controlled unclassified technical data with other certified US and Canadian contractors or US and Canadian military facilities.

NOTE:

The contractor must send a copy of the JCO-approved DD Form 2345 along with the requests for any of the above.

A3.6. Form 2345 Review Process. The JCO reviews a DD Form 2345 within 5 working days and takes one of the following actions based on its interpretation and confirmation of the information that the contractor provides:

A3.6.1. Certifies the contractor. The JCO:

- Enters a 7-digit certification number in section 7.
- Signs the form in sections 8 and 9.
- Mails the original to the contractor's data custodian.
- Sends the certified contractor a renewal notice 120 days before the certification expires.
Note: Certified contractors must submit a revised DD Form 2345 when the previous information becomes outdated (for example: changes in company ownership, company name, or data custodian). When the JCO approves the revised agreement, it initiates a new 5-year eligibility period.

A3.6.2. Returns the form for more information.

A3.6.3. Does not certify the contractor. The JCO:

- Sends a registered letter to the contractor, explaining why the certification was rejected.
- Tells the contractor how to appeal the decision.

Attachment 4

**SAMPLE DENIAL LETTER
TO PEOPLE WHO ARE NOT CERTIFIED US CONTRACTORS**

Dear Mr Jones:

The information that you requested on (date) is subject to control under Executive Order and export-control laws. We must deny your request under 5 U.S.C. 552(b)(3) and 10 U.S.C. 130 as implemented by Department of Defense Directive 5230.25 and Air Force Instruction 61-204.

If you decide to appeal this decision, write to us within 60 calendar days from the date of this letter. Include in the appeal your reasons for reconsideration, and attach a copy of this letter. Address your letter as follows:

(address of STINFO Officer)

Private individuals or enterprises must be Department of Defense certified US contractors before they can receive controlled technical data. Additionally, the information requested must relate directly to a legitimate business purpose for which the certification is granted. I have attached an information sheet describing the process you must follow to become a certified US contractor.

Please call (name, organization, phone number) if you have questions.

Sincerely,

Attachment 5

INFORMATION SHEET ON THE CERTIFIED US CONTRACTOR PROGRAM

A5.1. DoDD 5230.25 instituted a program to allow a private individual or business, called a certified US contractor,¹ to receive export-controlled technical data under certain conditions. One of the conditions is that the contractor must be certified in accordance with established DoD procedures. The US contractor must guarantee that:

A5.1.1. The individual who will act as recipient of the export-controlled technical data on behalf of the US contractor is a US citizen or a person admitted lawfully into the United States for permanent residence and is located in the United States.

A5.1.2. The data are needed to bid or perform on a contract with the Department of Defense or other US Government agency, or other legitimate business purposes² in which the US contractor is engaged, or plans to engage. The US contractor must describe sufficiently the purpose for which the data are needed to determine if subsequent requests for data are properly related to the business purpose.

A5.1.3. The US contractor acknowledges its responsibilities under US export-control laws and regulations (including the obligation, under certain conditions, to obtain an export license prior to the release of technical data within the United States) and agrees that it will not disseminate any export-controlled technical data in a manner that would violate applicable export-control laws and regulations.

A5.1.4. The US contractor agrees not to provide access to export-controlled technical data to people other than its employees or people acting on its behalf, without the permission of the DoD component that provided the technical data.

A5.1.5. To the best of its knowledge and belief, the US contractor knows of no person whom it employs who is acting on its behalf, who will have access to such data, who is debarred, suspended, or otherwise ineligible from performing on US Government contracts; or has violated US export-control laws or certification previously made to the DoD.

A5.1.6. The US contractor itself is not debarred, suspended, or otherwise determined ineligible by any agency of the US Government to perform on US Government contracts, has not been convicted of export-control law violations, and has not been disqualified under the provisions of this directive.

A5.2. The Defense Logistics Services Center (DLSC) in Battle Creek MI 49016-3412, certifies certified US Contractors. Those desiring certification should submit a DD Form 2345, **Export-Controlled DoD Technical Data Agreement**, to DLSC. You may obtain forms from the Navy Publications and Forms Center, 5801 Tabor Avenue, Philadelphia PA 19120-5099. Refer questions to DLSC at 1-800-352-3572.

¹Canadian contractors may be certified in accordance with this directive for technical data that does not require a license for export to Canada under section 1225.12 of the International Traffic in Arms Regulation and sections 379.4(d) and 379.5(e) of the Export Administration regulations by submitting an equivalent certification to the DoD.

²This does not require a contract with or a grant from the US Government.

Attachment 6

SAMPLE DENIAL LETTERS TO CERTIFIED US CONTRACTORS

A6.1. EXAMPLE 1. When the requested data are not related to the contractor's certification:

Dear Mr. Jones:

Your request of (date) for controlled, unclassified technical data is denied pursuant to Title 5 U.S.C. 552(b)(3) and Title 10 U.S.C. 130 as implemented by Department of Defense Directive 5230.25 and Air Force Instruction 61-204. We reviewed your request as a certified US contractor carefully and find that the data that you requested are not related to the purpose for which you are certified.

You may ask to be recertified by the Defense Logistics Services Center, Federal Center, Battle Creek, MI 49016-3412. If you decide to appeal this decision, write to us within 60 calendar days from the date of this letter. Include in the appeal your reasons for reconsideration, and attach a copy of this letter. Address your letter as follows:

(address of local STINFO Officer)

Please call (name, organization, phone) if you have questions.

Sincerely,

A6.2. EXAMPLE 2. When releasing the data for other than direct support of the Air Force and the release might jeopardize US technical or operational military advantages:

Dear Mr. Certified:

Your request of (date) for controlled, unclassified technical data is denied pursuant to 5 U.S.C. 552(b)(3) and 10 U.S.C. 130 as implemented by Department of Defense Directive 5230.25 and Air Force Instruction 61-204. We have reviewed your request carefully and have determined that releasing the data for other than direct support of the Air Force might jeopardize US technical or operational military advantages.

If you decide to appeal this decision, write us within 60 calendar days from the date of this letter. Include in the appeal your reasons for reconsideration, and attach a copy of this letter. Address your letter as follows:

(address of local STINFO Officer)

Please call (name, organization, phone) if you have any questions.

Sincerely,

Attachment 7

SAMPLE FREEDOM OF INFORMATION ACT (FOIA) DENIAL LETTER

(For requests for export-controlled technical data under FOIA from someone other than a certified US contractor.)

Dear Requestor:

This is in response to your Freedom of Information request of (date). The records that you request are exempt from disclosure because they contain unclassified data with military or space application for which an approval, authorization, or license would be required for its lawful export under Executive Order or export control law. Such data may be released in certain cases, however, to individuals or companies certified by the Department of Defense (DoD) as Certified US Contractors. Attached for your information is a description of this program.

The authority for this denial is in 5 U.S.C. 552(b)(3), 10 U.S.C. 130, and Air Force Instruction 61-204. The release of this information would jeopardize governmental interests in protecting technical information.

Should you decide to appeal to this decision, you must write to the Secretary of the Air Force within 60 calendar days from the date of this letter. Include in the appeal your reasons for reconsideration, and attach a copy of this letter. Address your letter as follows:

Secretary of the Air Force

THRU: (address of local FOIA office)

NOTE:

If this is a partial denial, add the following in a new paragraph if you are sending or will send copies of releasable records: We are attaching the releasable portion of these records. [or] We shall send the releasable portion of these records by separate letter.

Sincerely,

NOTE:

Prepare an original letter rather than a form letter or a form. Send by first class mail.

Attachment 8

NOTICE TO ACCOMPANY THE DISSEMINATION OF EXPORT-CONTROLLED TECHNICAL DATA

Export of information contained herein, which includes, in some circumstances, release to foreign nationals within the United States, without first obtaining approval or license from the Department of State for items controlled by the International Traffic in Arms Regulation (ITAR), or the Department of Commerce for items controlled by the Export Administration Regulation (EAR), may constitute a violation of law.

Under 22 U.S.C. 2778, the penalty for unlawful export of items or information controlled under the ITAR is up to 2 years imprisonment, or a fine of \$100,000, or both. Under 50 U.S.C., appendix 2410, the penalty for unlawful export of items or information controlled under the EAR is a fine of up to \$1,000,000, or five times the value of the exports, whichever is greater; or for an individual, imprisonment of up to 10 years, or a fine of up to \$250,000, or both.

In accordance with your certification that establishes you as a "certified US contractor," unauthorized dissemination of this information is prohibited and may result in disqualification as a certified US contractor, and may be used in determining your eligibility for future contracts with the Department of Defense.

The US Government assumes no liability for direct patent infringement, contributory patent infringement, or misuse of technical data.

The US Government does not warrant the adequacy, accuracy, currency, or completeness of the technical data.

The US Government assumes no liability for loss, damage, or injury resulting from manufacture or use for any purpose of any product, article, system, or material involving reliance upon any or all technical data furnished in response to the request for technical data.

If the technical data furnished by the Government will be used for commercial manufacturing or other profit potential, a license for such use may be necessary. Any payments made in support of the request for data do not include or involve any license rights.

Include a copy of this notice with any partial or complete reproduction of these data that are provided to certified US contractors.