

# Chapter 11.

## Miscellaneous Information

### Section 1. Tempest

**11-100. General.** TEMPEST is an unclassified short name referring to investigations and studies of compromising emanations. Compromising emanations are unintentional intelligence-bearing signals that, if intercepted and analyzed, will disclose classified information when it is transmitted, received, handled, or otherwise processed by any information processing equipment.

**11-101. TEMPEST Requirements.** TEMPEST countermeasures will be applied only in proportion to the threat of exploitation and the resulting damage to the national security, should the information be obtained by a foreign intelligence organization. It is the responsibility of the GCA to identify in writing what TEMPEST countermeasures may be required. The GCA will identify any TEMPEST requirements within the United States to the CSA for approval prior to imposing requirements for TEMPEST countermeasures upon their contractors. Contractors may not impose TEMPEST countermeasures upon their sub-contractors without GCA and CSA approval.

b. The Government is responsible for performing threat assessment and vulnerability studies when it is determined that classified information may be exposed to TEMPEST collection.

c. Contractors will assist the GCA in conducting threat and vulnerability surveys by providing the following information upon request:

- (1) The specific classification and special categories of material to be processed/handled by electronic means.
- (2) The specific location where classified processing will be performed.
- (3) The name, address, title, and telephone number of a point-of-contact at the facility where processing will occur.

**11-102. Cost.** All costs associated with applying TEMPEST countermeasures, when such countermeasures are imposed upon the contractor by a GCA, shall be recoverable by direct charge to the applicable contract. The GCA should provide TEMPEST shielding and shielded equipments GFE when such extreme countermeasures are deemed essential to the protection of the information being processed.

## Section 2. Defense Technical Information Center

**11-200. General.** The DoD operates certain activities to assist individuals and organizations in gaining access to scientific and technical information (STI) describing planned or on-going RDT&E efforts of the DoD.

a. The Defense Technical Information Center (DTIC) is the central point within DoD for acquiring, storing, retrieving, and disseminating STI to support the management and conduct of DoD research, development, engineering, and study programs.

b. DTIC is under the operational control of the Under Secretary of Defense for Acquisition and Technology. Its main facility is located at Cameron Station, Alexandria, VA. Other DTIC sites serve localized communities and special research interests through remote online service facilities.

### 11-201. DTIC Addresses.

**Defense Technical Information Center**  
Building 5, Cameron Station  
Alexandria, VA 22304-6145  
(703) 274-6434

**DTIC Albuquerque Regional Office**  
PL/SUL  
Aberdeen Avenue, S.E.  
Kirtland AFB, NM 87117-5776  
(505) 846-6797

**DTIC Boston Regional Office**  
5 Wright St., Bldg. 1103  
Hanscom AFB, MA 01731-3012  
(517) 377-2413

**DTIC Los Angeles Regional Office**  
222 N. Sepulveda Boulevard, Suite 906  
El Segundo, CA 90245-4320  
(213) 335-4170

**DTIC Dayton Regional Office**  
2690 C Street, Suite 4  
Building 22  
Wright-Patterson AFB, OH 45433-7411  
(513) 255-7905

**DTIC Manpower and Training Research**  
Information System, ATTN: DTIC-AM  
53355 Cole Road  
San Diego, CA 92152-7213  
(619) 553-7000

**11-202. User Community.** DTIC services are available to the DoD and its contractors and to other U.S. Government organizations and their contractors. Contractors may also become eligible for services under the Defense Potential Contractors Program.

**11-203. Registration Process.** All users are required to register for service. Registration, which is free, generally involves completing two forms which are available from DTIC as part of a registration kit.

a. DD Form 1540, "Registration for Scientific and Technical Information Services." This form shall be completed for each contract that authorizes use of DTIC services. This authorization is included in the Contract Security Classification Specification. The DD Form 1540 is submitted to DTIC through the sponsoring GCA for certification and approval. If a subcontract is involved, the DD Form 1540 is submitted through the prime contractor. The DD Form 1540 remains in force until completion of the classified contract or subcontract.

b. DD Form 2345, Militarily Critical Technical Data Agreement. Qualified contractors are eligible for access to militarily critical technical data after certification with Defense Logistics Services Center (DLSC) by completing the DD Form 2345. This DLSC certification is supplementary to registration with the DTIC. Upon certification with DLSC, the user also may be eligible for access to unclassified, militarily critical technical data from other DoD sources. All security criteria, including the need for a facility clearance, still must be met for the user to have access to the Defense RDT&E Online System (DROLS) or to obtain classified material.

**11-204. Safeguarding Requirements.** Classified information acquired from DTIC shall be safeguarded in accordance with the requirements of this Manual and with any restrictions that are marked on the material itself. The specific contract number that authorized the contractor access to the information shall be placed on each classified document. When the contract to which the DD Form 1540 applies is completed or terminated, the contractor shall either destroy or request retention for the material.

**11-205. DTIC Downgrading or Declassification Notices.** DTIC remarks downgraded or declassified paper documents to reflect such action only on the front and back covers and the title, first, and back pages. It is the responsibility of the recipient to complete any remarking required. Documents originally marked under the provisions of previous E.O.s may contain pages that do not bear any classification markings. Before extracting or reproducing the information from these pages, contractors should direct any questions they may have to the originator of the document.

**11-206. Questions Concerning Reference Material.**

Most material made available to contractors by DTIC and other distribution agencies is "reference material" as defined by this Manual. Therefore, the GCA that authorized the services of DTIC under a specific contract may not be in a position to provide the contractor with classification guidance for the reference material.

Classification jurisdiction always is the responsibility of the originating agency, or its successor, not necessarily the authorizing GCA. When a contractor requires classification guidance for reference material to prepare guidance for a subcontract or for other reasons and needs assistance in identifying the responsible department or agency, the CSA should be consulted.

**11-207. Subcontracts.** If a contractor awards a subcontract, that authorizes the subcontractor to use the services of DTIC and is expected to require access only to classified reference material, the Contract Security Classification Specification issued to the subcontractor shall show the highest category of classification required and a statement similar to the following: "Information extracted from classified reference material shall be classified according to the markings on such material. The DD Form 1540 prepared under this subcontract shall be forwarded through (name of prime contractor)."

### Section 3. Independent Research and Development Efforts

**11-300. General.** This Section provides special procedures and requirements necessary for safeguarding classified information when it is incorporated in contractors independent research and development (IR&D) efforts.

**11-301. Limitations.** Contractors frequently must use classified information in their IR&D efforts to effectively explore technological advancements and state-of-the-art improvements.

- a. Contractors are generally precluded from disclosing classified information to other cleared contractors in connection with an IR&D effort without the prior written approval of the agency that has jurisdiction over the information or the agency that provided the information to the contractor.
- b. DoD contractors shall not release or disclose classified information, under the jurisdiction of a non-DoD Agency to other cleared contractors in connection with an IR&D effort without the written approval of the non-DoD Agency.
- c. DoD cleared contractors may disclose SECRET and CONFIDENTIAL information, under the jurisdiction of a DoD contracting activity, to other DoD cleared contractors in connection with an IR&D effort unless specifically prohibited by the DoD in a Contract Security Classification Specification or other written notification.

**11-302. Information Generated Under an IR&D Effort that Incorporates Classified Information.** Under E.O. 12356, information that is in substance the same as information currently classified, requires a derivative classification. Therefore, information in a contractor's IR&D effort will require a derivative classification.

**11-303. Classification Guidance.** The releasing contractor may extract guidance appropriate for the IR&D effort from:

- a. An existing Contract Security Classification Specification that was previously furnished by a GCA in connection with performance of a classified contract;

- b. A final Contract Security Classification Specification that was issued in connection with retention of classified documents under a completed contract;
- c. A security classification guide obtained from DTIC;
- d. A classified source document.

*NOTE: The Department of Defense "Index of Security Classification Guides," and many of the listed security classification guides, are available to contractors who are registered with the DTIC. Contractors are encouraged to use the Index and the listed guides to obtain up-to-date security guidance for the classified information involved when developing guidance appropriate for their IR&D efforts.*

**11-304. Preparation of Security Guidance.** Contractors shall use the Contract Security Classification Specification to provide security guidance for the classified information released in their IR&D efforts.

**11-305. Retention of Classified Documents Generated Under IR&D Efforts.** Contractors may retain the classified documents that were generated in connection with their classified IR&D efforts for the duration of their facility clearance provided they have proper storage capability. Documents shall be clearly identified as "IR&D DOCUMENTS." A contractor's facility clearance will not be continued solely for the purpose of retention of classified IR&D documents without specific retention authorization from the GCA that has jurisdiction over the classified information contained in such documents. Contractors shall establish procedures for review of their IR&D DOCUMENTS on a recurring basis to reduce their classified inventory to the minimum necessary.