



***Basic
Foreign
Disclosure
Pocket Guide***

Fifth Edition

The information contained in this Pocket Guide, derived from FDE Solutions' foreign disclosure training seminars, does not certify an individual or organization to act as a designated disclosure authority (DDA)/foreign disclosure officer (FDO), or to disclose/release export-controlled information to a foreign government or international organization, or its representatives, without the approval of a DDA/FDO.

Each Pocket Guide segment is derived from existing Directives and Instructions. See www.fdesolutions.com, Disclosure Tools, for details.

TABLE OF CONTENTS

FOREIGN DISCLOSURE POINTS OF CONTACT	3
FOREIGN DISCLOSURE RULES OF THUMB	4
CORE DISCLOSURE CONCEPTS	6
FIVE DISCLOSURE CRITERIA	7
CUI DISCLOSURE CRITERIA	7
CMI DISCLOSURE CRITERIA	7
REQ FOR DISCLOSURE GUIDANCE (TEMPLATE)	8
PREPARING BRIEFINGS	9
DO'S & DON'TS OF FOREIGN TRAINING	10
PROCEDURES FOR SANITIZING DOCUMENTS	10
PEPS & FLOS	12
FOREIGN REPRESENTATIVE	12
HOST AND ESCORT RESPONSIBILITIES	13
BASIC DEFINITIONS	14
NOFORN	14
APPLICATION OF DISTRIBUTION STATEMENTS	15
USE OF "REL TO" FOR RELEASABLE MATERIAL	15
EIGHT NDP-1 CATEGORIES	16
PUBLIC DOMAIN	16
FOREIGN DISCLOSURE CONCEPTS	17
FALSE IMPRESSIONS DOCTRINE	17
WITHHOLDING AN ITEM FROM FOREIGN RELEASE	18
DEFENSE ARTICLES, SERVICES, & TECH DATA	18
WRITE FOR RELEASE	19
ABOUT FOREIGN DISCLOSURE & EXPORT SOLUTIONS	20

U.S. Marine Corps Foreign Disclosure Contacts:

Ms. Cindy Davis, HQMC (PP&O), Cats 1-7, 703-692-4342
NIPR: cynthia.l.davis@usmc.mil

SSgt Joshua Kirchem, HQMC (DIRINT), Cat 8, 703-614-1668
NIPR: joshua.kirchem@usmc.mil

Mr. Jeff Scribner, MCIA, Cat 8, 703-432-7336 (secure)
NIPR: j.scribner@mcia.osis.gov

Mr. Mike Ansley, MARCORSSYSCOM, Cats 2&3, 703-434-8978
NIPR: michael.a.ansley@usmc.mil

Mr. Gary Hanson, MARFORPAC, 808 477-8419 (DSN-315)
NIPR: gary.hanson@usmc.mil

Ms. Parker-McCullough, MARFORCOM, 757-836-1550
NIPR: betty.parkermccullough@usmc.mil

Ms. Kathy Fresia, II MEF, 910-451-1978
NIPR: katherine.fresia@usmc.mil

Mr. Bob Bandy, MARSOC, 910-451-2083
NIPR: robert.bandy@usmc.mil

Mr. Jim Rickard, MARFOREUR, DSN 314-431-2830
NIPR: james.rickard@mfe.usmc.mil

Mr. Carl (Chip) Loos, MARFORAF, DSN 314-431-2219
NIPR: carl.loos@mfe.usmc.mil

FOREIGN DISCLOSURE RULES OF THUMB™

Rule of Thumb Number 1 (Policy Rule):

If they don't own it or haven't signed a deal to buy it, or if there's no policy allowing it*, then they don't get it.™

(*Top-level disclosure policies are managed by Service HQ Disclosure Organizations and may require National-level coordination to execute. Ask your DDA for help, especially if classified information is proposed for disclosure where the receiving country is not buying the weapon, system, or equipment.)

Rule of Thumb Number 2 (Limited Information Rule):

Give 'em only exactly what they need, or what the situation requires.™

Rule of Thumb Number 3 (Past Precedent Rule):

If they got it before, they can get it again, but only if it hasn't changed.™

Rule of Thumb Number 4 (False Impressions Rule):

**Don't mention it, or offer it,
unless you know they can have it.**TM

Rule of Thumb Number 5 (Foreign Training Rule):

**If they obtain a new skill,
or improve an existing skill,
then it's training and it's not for free!**TM

Rule of Thumb Number 6 (Originator's Consent Rule):

**If they want it, but you didn't write it,
you need to obtain permission
from the person who did.**TM

Rule of Thumb Number 7 (Special Case Rule):

**There are exceptions to everything,
so if you think it's a good idea,
then ask a DDA.**TM

CORE DISCLOSURE CONCEPTS

NO COUNTRY IS "ELIGIBLE" TO RECEIVE ANY U.S. CLASSIFIED OR CONTROLLED UNCLASSIFIED MILITARY INFORMATION (CMI or CUI, respectively) BY VIRTUE OF NDP-1 (the NATIONAL DISCLOSURE POLICY MANUAL).

ALL DISCLOSURE DECISIONS FOR THE RELEASE OF CMI OR CUI ARE MADE ON A CASE-BY-CASE BASIS BY A DELEGATED DISCLOSURE AUTHORITY (DDA). AN ITEM'S CLASSIFICATION LEVEL (C, S, or TS) IS ONLY ONE FACTOR IN THIS DECISION, BUT IT IS NOT THE DRIVING OR DETERMINING FACTOR ALONE.

ONLY A DOD PUBLIC AFFAIRS OFFICER (PAO) MAY CERTIFY INFORMATION AS "PUBLIC DOMAIN". THE APPEARANCE OF INFORMATION ON THE INTERNET DOES NOT NECESSARILY IMPLY THAT A PAO HAS CERTIFIED IT AS PUBLIC DOMAIN.

** **UNCLASSIFIED** does not imply releasable.*

** **NDP-1 CLASSIFICATION LEVELS** do not imply information at or below a designated level is releasable.*

** **RELEASABLE** does not imply that any foreign representative may have access to information when there is no need-to-know.*

FIVE DISCLOSURE CRITERIA

ALL foreign disclosure decisions must meet the following five disclosure criteria:

1. The release must support U.S. foreign policy towards the intended recipient government, and toward other gov'ts in the region.
2. The release must not jeopardize U.S. military security or objectives.
3. The recipient government must possess the capability and intent to provide substantially the same degree of protection as the U.S.
4. The release must result in a clearly defined benefit to the U.S.
5. The release must be limited to that information minimally necessary to satisfy the purpose for which it is authorized.

CUI DISCLOSURE CRITERIA

- 5 Disclosure Criteria must be met
- Must have Originator's consent
- Must have all potential Stakeholder's consent
- The recipient must have a need-to-know
- The disclosure must be authorized by a DDA/FDO

CFI DISCLOSURE CRITERIA

- 5 Disclosure Criteria + CUI Disclosure Criteria
- The disclosure has been requested via Official Channels
- Must be in accordance with Service/CJCS/COCOM Policy
- Is within the scope of National Disclosure Policy
- Falls within the scope of command's Delegation of Disclosure Authority Letter (DDL), or forwarded up the chain of command, with a recommendation for resolution by a higher DDA/FDO

REQUEST FOR FOREIGN DISCLOSURE GUIDANCE (TEMPLATE)

1. Request Foreign Disclosure Guidance for the <oral/visual disclosure or documentary release> of <a general description of what is to be disclosed, e.g., technical system data for the AN/ABC-123> to representatives from the Government of <name of government> for <justification for the disclosure>.
 - A. The highest level of classified information proposed by this request is <TS/S/C>.
 - B. An FDD is requested due to the non-acquisition nature of the disclosure.
 - C. Request approval no later than <date>.
2. The NDP-1 categories and classification levels of information thought to be included in this requesting include: <list Cats & TS/S/C>
3. The specific information proposed for disclosure includes:
 - A. <Be specific here. What is going to be disclosed/released? Who "owns" it? What SMEs may need to be consulted by the DDA? If derived from multiple sources, do you have the multiple sources list? What will not be shown/released/discussed?>
 - B. <continue with additional paragraphs as required>
 - C. There <are or are not> past precedents for the disclosure of this information to <this or other foreign governments>. <Detail the past disclosure precedents if known.>
 - D. The information described above is limited to the minimum necessary to fulfill the purpose of the disclosure.
4. The U.S. operational goal served by this disclosure is <insert the goal, exercise, etc.>. This goal is endorsed and supported by <name of major command or flag/general officer supporting the request>. The equivalent benefit to the U.S. resulting from this disclosure includes <insert>.
5. Should this information be compromised, the impact to U.S. national security may be <detail as much as possible/known>. Compromise of this information <may or may not> cause U.S. technology to be killed, cloned, or countered.

(continued on next page)

6. (U) The actual transfer of information, if approved, will be performed by <detail how the transfer will comply with the Government-to-Government principle>. Transfers will only be made to recipients that have proper authority to receive the information for his/her Government.
7. (U) A record of transfer e-mail will be provided following the transfer which will detail the name of the recipient, the time and place of transfer, the exact information transferred, and any other feedback as may be required for disclosure purposes.

PREPARING BRIEFINGS

When submitting the briefing for a disclosure review by a DDA/FDO, include on a separate page all references and a multiple sources list, linking these to the briefing's content. Also include your speaking notes complete with talking points and key bullets. Tell the DDA/FDO who the intended audience is expected to be, their technical capabilities, and the four or five key points to be made by the briefing (the purpose of the disclosure). Finally, tell the DDA/FDO whether you want to distribute hard copies or just provide the brief as an oral/visual disclosure (and for classified meetings, whether or not you desire to allow note taking).

Any CMI notes taken by a foreign representative must be collected and forwarded to them via government-to-government channels (unless they possess a courier card or equivalent). All notes taken during a classified meeting should be assumed to be classified.

1. Disclose only necessary information.
2. Look closely at charts, graphs, and numbers. Engineering precision is normally not required.
3. In the briefing itself, do not include reference information (unless it is known to be releasable to everyone in your audience).
4. Briefing Title Slide or Slide #2 should say: "Hard copies of this briefing will (or will not) be provided." (per the DDA's guidance)
5. (*For classified briefings*) Briefing Slide #2 should also say: "Notes taken from this briefing are (or are not) authorized." (per DDA's guidance)

DO'S AND DON'TS OF FOREIGN TRAINING

Training is a defense service that is export-controlled and subject to foreign disclosure review. (ITAR/Arms Export Control Act)

- Do's:
- Train only to the limits of the foreign country's equipment or the applicable disclosure authorization (DDL)
 - Normally provide oral/visual training only
- Don'ts:
- Do not provide training for free
 - Do not transfer documents, unless specifically authorized by the export license or DDL
 - Do not volunteer extra information

PROCEDURES FOR SANITIZING DOCUMENTS

I. The disclosure of documents often requires text, charts, graphs, and even entire sections to be removed before being provided to foreign governments. This procedure is generally termed "sanitizing." It may be accomplished in a variety of ways:

A. Whenever possible, completely remove entire volumes, chapters, sections or paragraphs from the document. If more exact sanitizing is required, remove sentences, words, and graphics from the document. Exact sanitizing may result in a more precise document, but is labor-intensive and requires an extensive knowledge of the information being reviewed.

1. When hard-copy documents are sanitized, the proper procedure is to blank out the non-releasable information completely and then reproduce the page in its sanitized form. Use of this technique should not allow the reader to see non-releasable information. It is important that the reverse side of a sanitized page must also be reproduced if the intent is to keep the document flowing like a book. The sanitized pages are then substituted for the original pages. This is an expensive and time-consuming procedure.

2. Electronic documents may be edited, and then printed from the source computer file with the non-releasable portions of the document removed. There is some concern that electronically editing a computer file and then saving the edited file to a disk or CD -OM may not completely sanitize a document, because the recipient may have the technological capability to restore the original file from the sanitized version. Printing the edited file to paper is the safest means to deliver a sanitized electronic document.

B. Under no circumstances shall sanitizing be attempted by simply marking out non-

releasable portions alone (i.e., using pencil, ink, tape, etc.), without reproducing the page, since line-outs are not an effective means of removing information.

- C. In all cases, the table of contents, indices, lists of effective pages, etc., must be appropriately sanitized to remove references to deleted portions of a sanitized document. Additionally, reference lists, bibliographies, and distribution lists should be removed unless all of the documents identified have been reviewed and determined releasable. Requests for the disclosure of documents that are solely reference lists or bibliographies should normally be denied.
- D. A sanitized document shall add the subtitle "(Edited for *Country Name*)" or "REL TO USA, (Tri-graph), and the cover marking with the standard transfer, use and protect clause. Distribution Statements and Export Control Warnings should remain in place.

II. Under certain circumstance, some Services permit the casual mention of weapon or system names for weapons or systems that are not authorized for release when to remove such references would be resource intensive. This type of casual mention is generally unclassified and should reveal no system vulnerabilities, performance parameters, or specific variants released to foreign countries, and does not violate any Service or DoD policy concerning the mentioning of the weapon or system.

III. If the document contains non-releasable information and its removal is not feasible (e.g., it is impossible to eliminate the non-releasable content and still have the document serve the intended purpose), then the request for the disclosure of the document must be denied.

Note

Sanitizing instructions & foreign disclosure policies or limitations are not to be released. These represent U.S. Gov't policies and must not be discussed or disclosed to foreign representatives.

Caution

Documentary disclosures will be limited to that information which minimally satisfies the purpose of the disclosure. Gratuitous or extraneous disclosure of information is not permitted.

Warning!

Automatic Distribution of classified documentary material to foreign governments or representatives without a foreign disclosure

PEP's AND FLO's

<u>PEPs</u>	<u>FLOs</u>
one of THEM working for US	one of THEM working for THEM

Foreign Exchange personnel, regardless of rank or position, shall not at any time have unsupervised access to **SIPRNET** or be assigned certain watches, duties or billets that may allow unsupervised or inadvertent access to non-releasable information. In almost all cases exchange personnel may only have access to information releasable to their parent country and to which they have a bona fide "need-to-know".

FLOs cannot be assigned U.S. military billets or positions, and cannot be assigned tasks by U.S. officers, or act as a U.S. military command representative at any time.

U.S. Contact Officers overseeing PEPs and FLOs must:

- Inform personnel coming in contact with the PEP/FLO of their disclosure authorizations and limitations (e.g., conference calls, meetings, official travel, contractor interactions, etc.)
- Ensure PEP/FLO office location is clear of incidental disclosures
- Limit computer access to what is authorized in the DDL
- Ensure PEP/FLO e-mails properly document foreign national status

FOREIGN REPRESENTATIVE

A foreign representative is a person, regardless of citizenship, who represents a foreign interest in his or her dealings with the U.S. Government, or a person who is officially sponsored by a foreign government or international organization to act on its behalf. A U.S. national shall be treated as a foreign person when acting on behalf of a foreign interest.

Host/Escort Responsibilities During A Foreign Visit

1. Understand the definitions of Technical Data and Public Domain in this Guide.
 2. Comply with all physical security and base access procedures associated with "Incoming Visits by Non-U.S. Citizen and/or Foreign Persons."
 3. Inform all personnel that are, or may be involved in the visit, or come in contact with the foreign visitor, of the limitations on the release of controlled technical data or classified information to the foreign national visitor.
 4. Escort the Visitor(s) at all times.
 5. Perform a due diligence survey of the areas to be visited to ensure unauthorized disclosures do not occur, and obtain approval from the Security Department if access is required to classified or controlled areas.
 6. Ensure that the Visitor does not have unauthorized access to U.S. Government Classified Military Information (CMI), Controlled Unclassified Information (CUI), Technical data, or to Corporate/Proprietary information.
 7. Ensure that no transmissions of classified information or controlled technical data (CMI or CUI) takes place to the visitor without advance coordination and authorization from both the command's Security Department, and either an authorization from a Designated Disclosure Authority (DDA) or an approved State Department Export License.
 8. Review information to be disclosed to ensure that the data is within the scope of the disclosure authorization or export license. If access to controlled technical data or higher is required, then an approved Foreign Visit System (FVS) visit approval, with disclosure guidance, must also be provided.
 9. Immediately report all incidents or suspected incidents of compromise, or improper information requests from the visitor, to the Security Department.
 10. Contact the Security Officer if you have any questions relating to the visit.
-

The United States Government has specific regulations for all DOD Commands and contractor facilities that govern the access of Foreign Persons. A "Foreign Person" is a person who is not a U.S. Citizen, a lawful permanent resident or a protected individual. A Foreign Person includes, but is not limited to:

- 1) A U.S. Citizen who represents any foreign entity, such as a foreign corporation, business association, partnership, trust society, or any other group that is not incorporated or organized to do business in the U. S.
- 2) An International Organization representative (such as NATO)
- 3) A Foreign Government representative, or a representative from any agency or subdivision of a foreign government, (e.g., embassy or diplomatic mission)

BASIC DEFINITIONS

- ** DISCLOSURE: To transmit or confer information in any way
- ** ORAL/VISUAL DISCLOSURE: To show them, tell them, and let them use it, but not to give it to them
- ** DOCUMENTARY RELEASE: To give it to them
- ** CMI: Classified Military Information (C, S, TS)
- ** CUI: Is a general term, not an official classification. It includes:
 - Freedom of Info. Act (FOIA)-exempt material with a military or space application
 - Material covered by a Distribution Statement (Technical Publications)
 - May be labeled "For Official Use Only" by DoD
 - Includes DoD information that a PAO has not yet deemed "public domain"
- ** ITAR: Int'l Traffic in Arms Regulations (22 CFR Parts 120-130)

NOFORN

NOFORN is not a CMI distribution limitation, but an intelligence product marking. NOFORN material is not releasable under any circumstances. Conversely, the absence of a NOFORN marking does not imply that an item is automatically releasable.

In order for NOFORN material to be released, it must be reviewed, possibly sanitized, and then authorized for release. Only the original classification authority (OCA) may authorize modifications, changes in caveat markings, and release. If authorized by the OCA, the material's marking may be changed from NOFORN to REL TO.

APPLICATION OF DISTRIBUTION STATEMENTS

Distribution Statements are used to denote the extent to which documents are available for distribution, release, and dissemination without additional approvals or authorizations. If disclosure is requested beyond the limits of the Statement, it will state where these approvals may be obtained. They apply to engineering drawings, standards, specifications, tech manuals, blueprints, drawings, plans, instructions, computer software and documentation, and other technical information that can be used or be adapted for use to design, engineering, produce, manufacture, operate, repair, overhaul, or reproduce any military or space equipment or technology concerning such equipment. They are used for both CMI & CUI. Distribution Statements DO NOT apply to crypto, COMSEC, COMINT or ELINT information. (See DoD Directive 5230.24 for more details.)

Commonly used Distribution Statements are:

- A — Approved for Public Release ("public domain")
- B — U.S. Gov't Agencies only (not including support contractors)
- C — U.S. Gov't Agencies and their contractors
- D — U.S. DoD and DoD contractors only
- E — DoD Components only
- F — Dissemination only as directed
- X — U.S. Gov't Agencies and private entities eligible for export-controlled technical data

USE OF "REL TO" MARKING TO IDENTIFY RELEASABLE MATERIAL

The marking "REL TO" is an authorized disclosure marking. It may be applied to information disclosed on a oral/visual basis or hard copy release. To use this marking, the cover and each page and paragraph must be marked with the trigraph of the countries or organizations to whom the disclosure is made (e.g., SECRET REL TO USA, AUS, NATO). If the top and bottom security classification marking on a page applies to all information contained within a page, then the paragraph portion markings for that page may be abbreviated to "S//REL" (as an example).

EIGHT NDP-1 CLASSIFIED INFORMATION CATEGORIES

(Classification level (C, S, or TS) is a subset of each category.)

Categories (CAT)

CAT 1: Pubs, Tactics, Training (not weapons specific)

CAT 2: "Stuff" (Hardware, Software, & Weapons-Related Information)

CAT 3: Applied R&D

CAT 4: Manufacture and Production Information

CAT 5: Combined Ops, Plans, Exercises & Readiness

CAT 6: Order Of Battle (Tactical Data Picture, AOR only as necessary)

CAT 7: NORAD Information

CAT 8: Military Intelligence

PUBLIC DOMAIN

Information certified for public release by a DoD Public Affairs Officer (PAO), an empowered company representative (for unclassified Company-proprietary information), or DoD material marked as "Distribution Statement A." An item's appearance on the Internet does not, by itself, certify that it is officially "public domain." Per the ITAR (§120.11), public domain constitutes published information generally available to the public through sales at newsstands and bookstores; unrestricted subscriptions; second class mail; available at libraries or through the Patent Office; public distribution at conferences, seminars, meetings, etc.; or through fundamental-level research at accredited science and engineering institutions of higher learning.

FOREIGN DISCLOSURE IS BASED ON THESE CONCEPTS

Basic Foreign Disclosure Principles

Limit Access (Need-To-Know)

Content Protect (to the same degree as the U.S.)

Governing Laws (Provides Legal & National Authority)

Arms Export Control Act (AECA): governs the export of defense articles and services

Executive Order 12958: establishes the Executive Branch's Classified Security Information system

National Security Decision Memorandum (NSDM) 119: core national policy governing foreign disclosure

Fundamental Conditions for All Foreign Disclosures

No Third Party TRANSFERS (without U.S. consent)

No USE of the information beyond the intended purpose

Afford the same degree of PROTECTION as the U.S.

Government-to-Government Principle

Releasing or exporting information is a U.S. Gov't decision

All TRANSFERS must be through official channels (military postal service or government courier service), or through other channels approved by both governments

FALSE IMPRESSIONS DOCTRINE

Before a DOD organization enters into any initiative with a foreign government that will entail the eventual disclosure of any CMI or CUI, the organization shall obtain **prior disclosure authority** sufficient to provide all the information of the type and at the classification level that is known or anticipated for the life of the program or initiative before discussing the program or initiative with a foreign representative.

WITHHOLDING AN ITEM FROM FOREIGN RELEASE

The proper way for a non-intelligence item to be withheld from foreign disclosure is to mark the item "Release to Foreign Nationals Is Not Authorized" (or for the original classification authority to withhold authority to disclose the information when requested).

DEFENSE ARTICLES, SERVICES, & TECHNICAL DATA

**** A DEFENSE ARTICLE** means any item or its related technical data that is created or developed mainly for a military or defense purpose. This includes anything recorded or stored in any physical form, models, mock-ups or other items that reveal technical information directly relating to a defense article. (See ITAR Sec. 120.6)

**** A DEFENSE SERVICE** means any assistance provided to foreign persons, whether in the U.S. or abroad, in the design, development, engineering, manufacture, production, assembly, testing, repair, maintenance, modification, operation, demilitarization, destruction, processing or use of defense articles. Defense Service also includes military training of foreign units and forces, including formal or informal instruction, regardless of the location, or by correspondence courses, technical, educational, or information publications and media of all kinds, training aids, orientations, training exercises, and military advice. (See ITAR Sec 120.9)

**** TECHNICAL DATA** means (See ITAR Sec 120.10):

- (1) Information which is required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of a defense article. This includes information in the form of blueprints, drawings, photographs, plans, instructions and documentation.
- (2) All classified information relating to a defense article or service.

WRITE FOR RELEASE

1. Determine the recipient country(ies), the "target" country (if applicable) and subject matter, and NDP-1 categories/classification levels involved. Then consult the DDA/FDO/FDR to determine if there is disclosure authority to write the product.
2. Check all available resources for unclassified open-source information, or unclas multi-national publications, that can be used to meet the purpose of the disclosure. For classified info, try to find information already marked "REL TO", then unclassified information (or "RELIDO" (Releasable by Information Disclosure Official) for Cat 8), then NOFORN as a last resort. Use footnotes or endnotes to indicate the where the information or data comes in your product from if your command did not generate it yourself (ex., derived from NGA satellite product ___).
3. Write the product. Ensure that the DDA/FDO can tell what is original U.S. content and what is proposed as releasable text. Be consistent in the way that REL TO is used; either use it throughout as Proposed Releasable Text, or use it as Already Releasable Text. Don't mix the two. Make sure to delete all references to sources, other documents, and methods of collection in proposed releasable text.

There are generally two options for writing a releasable product:

 - a. Write a U.S. Only product (unclassified or marked NOFORN (Cat 8 only)), and then write a second Proposed REL TO version; or
 - b. Use a "Tear Line" to separate the intended recipients for each portion of the product. This is generally used for e-mails or messages. For example:
 - BEGIN TEAR LINE SECRET//NOFORN — followed by S//NF content
 - BEGIN TEAR LINE S//REL USA, XYZ — followed by S//REL XYZ content
 - BEGIN TEAR LINE S//REL USA, ABCD — followed by S//REL ABCD content
4. If possible, obtain the consent of all of the originators of the material obtained from other sources used in the document, as well as other offices or commands that may have an interest in the material, prior to sending the proposed text to the DDA/FDO for approval. Send all consenting e-mails as an attachment.
5. Send the proposed product to the DDA/FDO. When seeking approvals, make the DDA's/FDO's job as easy as possible by: (a) Use SIPRNET request forms if available; (b) Provide any proposed REL text if you are seeking to release NOFORN content; (c) Attach all original source documents used to develop your text and clearly indicate the sections used to write your product; and (d) Specify a due date.
6. Post the approved product for release on the appropriate network (for electronic documents) or distribute them via official government-to-government channels.

About Foreign Disclosure & Export Solutions

The Foreign Disclosure and Export Solutions Corporation, the creators of this Pocket Guide, provides expert training and consulting services to private companies and government agencies on matters relating to military technology transfer, international military cooperative programs, and export licensing of U.S. Munitions List items to friendly and allied nations of the United States. Their consultants use their prior foreign disclosure and export licensing government experience to assist their clients in properly expressing and presenting their information to disclosure officials and government reviewers in order to obtain the client's most advantageous outcome.

The information contained in this Pocket Guide is derived from the company's foreign disclosure seminars. These how-to seminars set the standard for the training of personnel that interface with foreign representatives. We encourage all persons using these Guides to attend a seminar in order to more effectively understand and use the information contained herein. For details about these seminars, go to <http://www.fdesolutions.com>.

For more information, or to recommend additions or changes to this Pocket Guide, please contact the Foreign Disclosure & Export Solutions Corporation.

Foreign Disclosure & Export Solutions Corporation
12962 Pinecrest View Ct.
Oak Hill, VA 20171-2644

(703) 860-8112

<http://www.fdesolutions.com>

info@fdesolutions.com