U.S. Department of Energy

National Energy Technology Laboratory

PROCEDURE

P 471.2-1

DATE: 2/24/03

SUBJECT: CONTROLLING SENSITIVE UNCLASSIFIED INFORMATION

1. PURPOSE. This Procedure shall document the security control measures practiced at NETL to prevent the inadvertent release of sensitive unclassified information (SUI) to any extent not authorized by statute, regulation, or DOE directives.

2. CANCELLATION. None.

3. REFERENCES.

   a. DOE Order 471.2, Information Security Program.

   b. FAR 52.227-14, Rights in Data General.

   c. Draft DOE Order 471.X, Identifying and Protecting Official Use Only Information.

   d. Draft DOE Manual 471.X-X, Manual for Identifying and Protecting Official Use Only Information.

   e. Draft DOE Guide 471.X.X, Guide to Identifying Official Use Only Information.

4. DEFINITIONS.

   a. Designated Secured Area -- Designated secured area is a location defined by the NETL Safeguards and Security Officer in which SUI can be stored for use or retention. An example would be a file drawer that can be locked within an office or work area.

   b. Export Controlled Information (ECI) -- ECI is technical information that cannot be exported unless licensed by the Department of State, Department of Commerce, or Nuclear Regulatory Commission. Examples of ECI are specific details of design, production, or use of technology that has military or national security applications. Employees are directed to consult with the Export Compliance Officer (currently the Security Program Manager) if they believe they have ECI.

INITIATED BY: Office of Business and Logistics
NO. OF PAGES/ATTACHMENTS: 6 pages, 4 attachments

c. Human Resource Information -- Human resource information is a type of official use only information.

d. In Use -- In use is a term that signifies that an NETL employee who is authorized to access SUI (i.e., has a "need to know" and as defined by this Procedure) is physically present when SUI is not in a designated secured area. That is the SUI is not left unattended and subject to disclosure to an unauthorized source.

e. Need-to-Know -- Sensitive unclassified information shall only be disseminated to persons acting in an official capacity to NETL that have a need-to-know the contents of the information to perform their official duties.

f. NETL Custodian -- NETL custodian is an employee that has sensitive unclassified information in their possession or control. Examples include, but are not limited to, Contracting Officers (CO), Contract Specialists, R&D personnel, or Contracting Officer Representatives (COR).

g. Official Use Only (OUO) Information -- Official use only information is information created within the U.S. Government (e.g., NETL or any other Government organization) that is to be safeguarded from loss, unauthorized disclosure, or misuse to protect Government or employee interests. Government employees may designate documents as OUO (refer to Attachment 2). Examples include, but are not limited to, personnel information, security plans, preliminary budget projections, contract files, technical data, etc.

To be identified as OUO, information must be unclassified; fall under at least one of eight Freedom of Information Act (FOIA) exemptions (Attachment 1); and be reasonably expected to cause damage to governmental, commercial, or private interests if disseminated to persons who do not need the information to perform their official duties or other DOE-authorized activities. OUO information will be for the purposes of this Procedure and subject to withholding from public disclosure under the criteria of the Freedom of Information Act (FOIA).

h. Proprietary Information -- Proprietary information is information or data of any type provided to NETL or an NETL employee by an external entity that has the legal right to protect such information or data from disclosure. Proprietary information is required to be marked with an appropriate legend. Examples of proprietary information include, but are not limited to, company financial data, insurance coverage, cost information, proprietary technical data, limited rights data, and restricted computer software.

i. Protected Information -- Protected information is trade secret type information protected from release for a limited period of time under the terms of an agreement (contract, financial assistance, or CRADA) that does not meet the definitions of proprietary and OUO information. Examples of protected information include, but are not limited to, EPACT protected information, Clean Coal protected information, power plant improvement initiative protected information, Clean Coal Power Plant initiative protected information, and CRADA protected information.

j. Sensitive Unclassified Information (SUI) -- SUI is unclassified information that includes either (1) proprietary information (owner is external to NETL), (2) official use only information (information created within the U.S. Government, i.e., NETL), and (3) protected information (information that has restricted disclosure that is not defined as proprietary or OUO.

k. Sensitive Unclassified Information List -- Critical and sensitive information list (SUIL) is a general listing of the physical areas within NETL where SUI may be present.

5. QUALITY CONTROL. This Procedure shall be revised as needed to ensure compliance with prevailing laws, regulations, DOE directives, or to facilitate the accomplishment of the NETL mission.

6. RESPONSIBILITIES.

a. The Deputy Director of Operations shall:

(1) Review and approve this Procedure.

b. The Security Program Manager shall:

(1) Provide oversight on the administration of this Procedure.

(2) Maintain this Procedure.

(3) Maintain the sensitive unclassified information list (SUIL).

c. Safeguards and Security Officer shall:

(1) Define designated secured areas.

(2) Provide for employee awareness of and training on this Procedure.

d. NETL Employees shall:

(1) Scrutinize information to determine if it should be controlled as SUI.

(2) Place the appropriate marking on OUO (Attachment 2).

(3) Not have in their possession SUI for which they are not authorized or have a need-to-know.

(4) Not disclose SUI except as authorized and in accordance with this Procedure.

7. TRAINING REQUIREMENTS. The NETL Safeguards and Security Office will provide annual training to all NETL employees on the requirements of this Procedure.

8. DOCUMENT CONTROL. This Procedure will be maintained by the NETL Security Program Manager.

9. PROCEDURE.

a. General procedures for identification of SUI:

(1) Proprietary information and protected information shall be clearly identified per the terms defined within the agreement by the provider and verified by the cognizant NETL custodian. Documents not in compliance shall, in coordination with the NETL Patent Attorney, be returned to the provider with instructions to identify and mark the information per the terms of the agreement.

(2) Proprietary information not subject to a formal agreement shall be returned to the provider with instructions to mark the information with an appropriate legend.

(3) Official use only information shall be marked by the NETL custodian as per the requirements of Attachment 2.

(4) All Human Resource information is considered OUO information unless otherwise determined in accordance with applicable laws and regulations. Human Resource information is exempt from the marking requirements for OUO information.

(5) Protected information (CRADA information) generated by NETL shall be marked according to the terms of the CRADA.

b. The NETL custodian possessing SUI is responsible for determining the recipient's need-to-know.

(1) For dissemination of SUI to NETL Federal employees, it is recommended, but not required, that the NETL custodian document the need-to-know. This documentation shall be kept in the designated secured area preferably attached to the referenced SUI.

(2) For the dissemination of SUI to non-NETL Federal employees or non-Federal employees, the NETL custodian shall use the procedure detailed in Attachment 3.

(3) Transmission of SUI by NETL custodians must be consistent with Attachment 4 of this Procedure.

(4) An important point with respect to dissemination of SUI is that compliance with this Procedure does not relieve NETL employees of the responsibility to comply

with Export Control Regulations (i.e., Department of Commerce or other Government regulations that control the dissemination of information to entities outside of the U.S.).

c. SUI shall be stored in a designated secured area when not in use. A locked office, a locked file cabinet, or locked file drawer, accessible only by the NETL custodian, can be used as a designated secured area.

Other types of locations require the approval of the NETL Safeguards and Security Officer (SSO) by using the following procedure:

The NETL custodian sends an e-mail to the SSO requesting a designated secured area that includes the following information:

- Location of the secured area.
- Description of the storage devise for SUI.

The NETL SSO will arrange for the inspection of the designated secured area. The NETL SSO will respond with an e-mail upon approval of the designated secured area.

d. NETL employees shall only take control of SUI if they have a need-to-know and they have been granted access to the information by the NETL custodian in control of the information.

e. NETL employees shall report to their supervisor, persons in possession of SUI who are not authorized or who do not have a need-to-know.

f. Employees may be subject to disciplinary or legal action due to improper handling of SUI or if found to be in possession of SUI in the absence of a need-to-know in accordance with applicable statutes, regulations, and procedures.

g. SUI shall be disposed of either by burning or shredding or as otherwise set forth by agreement.

10. ATTACHMENTS.

a. Attachment 1 -- Freedom of Information Act Exemptions (2 through 9).

b. Attachment 2 -- Official Use Only Markings.

c. Attachment 3 -- Disclosure and Change in Status of SUI.

d. Attachment 4 -- Transmission of Sensitive Unclassified Information.

_____
Associate Director, OBL

ATTACHMENT 1

FREEDOM OF INFORMATION ACT EXEMPTIONS 2 THROUGH 9

1. **Exemption 2: Circumvention of Statute**

   a. Statutory Text. Exemption 2 concerns information "related solely to the internal personnel rules and practices of an agency."

   b. Discussion. Exemption 2 protects information related to internal agency procedures, practices, and guidelines and applies to information that could benefit someone who is attempting to violate a law or agency regulation and avoid detection. Information may be OUO under Exemption 2 if its disclosure would allow a statute or agency regulation to be circumvented.

   c. Examples.

      (1) General guidelines for conducting investigations.

      (2) Vulnerability assessments.

      (3) Inspection and appraisal procedures.

      (4) Testing materials used to evaluate personnel for promotion, transfer, or demotion.

      (5) Unclassified (and uncontrolled) portions of information classification and control guidance.

      (6) Agency computer access codes.

2. **Exemption 3: Statutory Exemption**

   a. Statutory Text. Exemption 3 concerns information "specifically exempted from disclosure by statute . . . , provided that such statute (a) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue or (b) establishes particular criteria for withholding or refers to particular types of matters to be withheld."

   b. Discussion. Exemption 3 covers information that is explicitly prohibited from disclosure by a statute passed by Congress. Within DOE, the Atomic Energy Act, which is the basis for the formal control of restricted data, formerly restricted data, and UCNI, is an Exemption 3 statute, but these types of information are already subject to formal control systems and, therefore, are not also designated as OUO. However, there are other statutes that meet the requirements of this exemption for which there are no formal control systems in place. Information generated under those statutes may be OUO. Basing an OUO determination on an Exemption 3 statute is very complex and requires

interpretations of statutory language and case law. Therefore, its use should be limited to those cases where appropriate statute-specific guidance is available (e.g., from your local general counsel).

Examples.

(1) 15 U.S.C. 3710a(c)(7)(B) -- Federal Technology Transfer Act. This statute requires a Federal agency to protect any commercial and confidential information that results from a Cooperative Research and Development Agreement with a non-Federal party for a period of 5 years after its development. This Exemption 3 statute essentially extends the Exemption 4 concept of commercial and proprietary information to Government information. (See next paragraph for a discussion of Exemption 4.)

(2) Other Statutes. Many other statutes also explicitly prohibit disclosure of information; therefore, it is impossible to provide a definitive list. The following list of statute provisions/sections governing the protection/disclosure/confidentiality of information is provided to show the broad range of information that may be exempt under statute and, therefore, may be identified as OUO. (Most of these statutes do not apply to DOE.)

- 7 U.S.C. 12, Commodity Exchange Act.
- 8 U.S.C. 1202(f), Immigration and Nationality Act.
- 10 U.S.C. 130, Technical Data Statute (Department of Defense).
- 13 U.S.C. 8(b) and 9(a), Census Act.
- 15 U.S.C. 2055(a)(2), Consumer Product Safety Act.
- 18 U.S.C. 2510-20, Omnibus Crime Control and Safety Check Act.
- 22 U.S.C. 3104(c), International Investment Survey Act of 1976.
- 26 U.S.C. 6103, Internal Revenue Code.
- 35 U.S.C. 122, Patent Act.
- 45 U.S.C. 362(d), Railroad Unemployment Insurance Act.

3. **Exemption 4: Commercial/Proprietary**

a. Statutory Text. Exemption 4 concerns "trade secrets and commercial or financial information obtained from a person and [that is] privileged or confidential."

b. Discussion. Exemption 4 protects the interests of both the Government and persons submitting information to the Government. This exemption encourages commercial entities to voluntarily submit useful commercial or financial information to the Government and provides the Government with some assurance that the submitted information is reliable. In some cases, it appears that some overlap exists between Exemption 4 and Exemption 5 (see next paragraph for a discussion of Exemption 5). However, the distinction is that Exemption 4 applies to information generated by a company and provided to the Government whereas Exemption 5 applies to Government-generated information. Two broad categories of information are covered by this exemption: (1) trade secrets and (2) commercial or financial information.

(1) Trade Secrets. The definition of "trade secret" that has been adopted by the courts is "a secret, commercially valuable plan, formula, process, or device that is used for the making, preparing, compounding, or processing of trade commodities and that can be said to be the end product of either innovation or substantial effort." Thus, a direct relationship between the trade secret and the production process must exist. General information about a product's physical appearance or performance characteristics is not covered by this exemption unless such information would actually reveal the formula or process itself.

(2) Commercial or Financial Information. The second category of information is related to trade secrets but concerns information that is (a) commercial or financial, (b) obtained from a person, and (c) privileged or confidential. A general description of what is meant by each of these items is as follows:

(a) Commercial or Financial. Information is considered commercial if the person submitting it has a commercial interest in it. Information submitted by a nonprofit entity may also be considered commercial information. Financial information includes economic data generated solely by a corporation or other business entity, but it may also apply to personal financial information.

(b) Obtained from a Person. The term "person" refers to a wide range of entities that includes one individual, a corporation, a state government, a foreign government, or a Native American tribe or nation. However, it does not include the Federal Government; therefore, information generated by the Federal Government is not considered to be "obtained from a person" unless the product is merely a summary or reformulation of information supplied by entities from outside the Government.

(c) Privileged or Confidential. The term "privileged" extends the privileges covered under Exemption 5 for Government information to private sector information. To be considered "confidential," the information must meet one of the following tests: if submission of the information is required by the Government, the information may be protected if disclosure would (1) impair the Government's ability to obtain the information in the future

or (2) would cause substantial harm to the competitive position of the person submitting the information. If submission of the information is voluntary on the part of the submitter, the information may be protected if the submitter would not customarily release such information to the public.

c. Examples.

(1) Commercial or financial information received in confidence in connection with bids, contracts, or proposals and other related information received in confidence, such as trade secrets; inventions; discoveries; foreign ownership, control, or influence information; or other proprietary data.

(2) Statistical data and commercial or financial information concerning contract performance, income, profits, losses, and expenditures, if offered and received in confidence from a contractor or potential contractor. This includes business sales statistics, research data, technical designs, customer and supplier lists, overhead and operating costs, and information on financial condition.

(3) Sensitive information included in personal statements given in the course of inspections, investigations, or audits when such statements are received in confidence from the individual and retained in confidence because they reveal trade secrets or commercial or financial information normally considered confidential or privileged.

(4) Information dealing with scientific and manufacturing processes or developments concerning technical or scientific data or other information submitted with a contract proposal or as part of a report while the contract is in progress.

4. **Exemption 5: Privileged Information**

a. Statutory Text. Exemption 5 concerns "interagency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency."

b. Discussion. Exemption 5 protects privileged information that is based on statute or case law. The three primary privileges are (1) deliberative process privilege, (2) attorney work-product privilege, and (3) attorney-client privilege.

(1) Deliberative Process Privilege. This privilege is the most frequently used privilege under Exemption 5, and its purpose is to prevent injury to the quality of agency decisions. The bases for this privilege are:

(a) To encourage open, frank discussions on matters of policy between subordinates and superiors;

(b) To protect against premature disclosure of proposed policies before they are finally adopted; and

(c) To protect against public confusion that might result from disclosing reasons and rationales that were not ultimately the grounds for an agency's action. To apply the deliberative process privilege, the following fundamental requirements must be met:

- The communication must be predecisional (i.e., it must occur before a final decision is made). Note: A document containing recommendations or suggestions that were not implemented or adopted may still be OUO under Exemption 5 after a final decision is made.

- The communication must be deliberative (i.e., make recommendations or express opinions on legal or policy matters).

(2) Attorney Work-Product Privilege. This privilege protects documents and other memorandums prepared by an attorney in contemplation of litigation.

(3) Attorney-Client Privilege. This privilege protects confidential communications between an attorney and his or her client concerning a legal matter for which the client has sought professional advice.

c. Examples.

(1) Letters, memorandums, issue papers, reports, etc., that contain advice, opinions, or recommendations on new or revised Government decisions and policies.

(2) Advice, suggestions, evaluations, or recommendations prepared on behalf of DOE by individual consultants, boards, committees, councils, groups, panels, conferences, commissions, task forces, or other similar groups.

(3) Evaluations of contractors and their products and services by DOE personnel.

(4) Information of a speculative, tentative, or evaluative nature concerning proposed plans to procure, lease, or otherwise acquire and dispose of materials, real estate, facilities, or functions when such information would provide undue or unfair competitive advantage to private personal interests or would impede legitimate Government functions.

(5) Trade secret or other confidential research, development, or commercial information owned by the Government where premature release is likely to affect the Government's negotiating position or other commercial interests. (Note: Exemption 5 applies here because the information is owned by the Government, not a private company.)

(6) Information that is exchanged among DOE personnel and within and among agencies in preparation of anticipated administrative proceedings by an agency or litigation before any Federal or state court and information that qualifies for attorney-client privilege.

5. **Exemption 6: Personal Privacy**

a. Statutory Text. Exemption 6 concerns "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy."

b. Discussion. Exemption 6 protects personal information related to a specific individual that, if disclosed, might cause an individual personal distress or embarrassment.

c. Examples.

(1) Personal details about a Federal employee (e.g., social security number, citizenship data, date of birth).

(2) Intimate details of an individual's life (e.g., marital status, religious affiliation, legitimacy of children, sexual inclinations or associations, medical conditions, criminal history, financial data).

(3) Personnel matters in which administrative action, including disciplinary action, may be taken.

6. **Exemption 7: Law Enforcement**

a. Statutory Text. Exemption 7 concerns "records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information:

(1) Could reasonably be expected to interfere with enforcement proceedings,

(2) Would deprive a person of a right to a fair trial or an impartial adjudication,

(3) Could reasonably be expected to constitute an unwarranted invasion of personal privacy,

(4) Could reasonably be expected to disclose the identity of a confidential source, including a State, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and in the case of a record or information compiled by a criminal law enforcement authority in the course of a criminal investigation, or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source,

(5) Would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or

(6) Could reasonably be expected to endanger the life or physical safety of any individual."

b. Discussion. Exemption 7 protects information compiled by an agency with the authority to enforce civil statutes, criminal statutes, and statutes authorizing administrative proceedings. It covers information compiled for law enforcement purposes regardless of the format of the document or how and where the document may be filed. Exemption 7 protection is also extended to manuals that contain sensitive information about the law enforcement procedures followed by an agency charged with law enforcement responsibilities. The examples in the paragraph below identify easily understood types of information that may be considered as OUO; however, because this exemption has so many qualifiers, it is suggested that caution be used when basing an OUO determination on this exemption.

c. Examples.

(1) Statements of witnesses and other material developed during the course of an investigation and all materials prepared in connection with related Government litigation or adjudicative proceedings.

(2) The identity of firms or individuals being investigated for alleged irregularities involving contracting with DOE when no indictment has been obtained or no civil action has been filed against them by the United States.

(3) Information obtained in confidence, expressed or implied, in the course of a criminal investigation by a criminal law enforcement agency or a lawful national security intelligence investigation conducted by an authorized agency or office within DOE. National security intelligence investigations include background security investigations and those investigations conducted for the purpose of obtaining affirmative or counterintelligence information.

(4) Information from which a confidential source may be identified regardless of whether the source is an individual or an institution.

(5) Law enforcement manuals and guidelines describing specific procedures followed by an agency charged with law enforcement responsibilities.

(6) Information concerning homemade weapons that could assist a criminal element and might result in harm to individuals or property.

7. **Exemption 8: Financial Institutions**

a. Statutory Text. Exemption 8 concerns information "contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions."

b. Discussion. Exemption 8 protects frank evaluations of a financial institution's stability that might undermine the public's confidence in the institution or the relationship between financial institutions and supervisory agencies.

c. Examples.

(1) Bank examination reports.

(2) Documents related to bank examination reports (e.g., discussions of findings, follow-up actions).

8. **Exemption 9: Wells**

a. Statutory Text. Exemption 9 concerns "geological and geophysical information and data, including maps, concerning wells."

b. Discussion. Exemption 9 is rarely used but protects well information of a technical or scientific nature.

c. Example. Number, location, and depth of proposed uranium exploration drill holes.

ATTACHMENT 2

1. OFFICIAL USE ONLY MARKINGS

The employee making the determination that a document is to be handled as OUO must include both the applicable FOIA exemption number and the related category name on the following marking and ensure that the marking is placed on the front of the document containing OUO information:

OFFICIAL USE ONLY

May be exempt from public release under the Freedom of Information Act (5 U.S.C. 552), exemption number and category:

_____

Department of Energy review required before public release

Name/Org: _____ Date: _____

2. OFFICIAL USE ONLY INFORMATION PAGE MARKING

This marking (shown in bold below) shall be placed at the bottom of the first page of a document containing official use only information and on each page of the document that the SUI appears.

OFFICIAL USE ONLY

3. MARKING SPECIAL FORMAT DOCUMENTS

Special format documents (e.g., photographs, viewgraphs, films, magnetic tapes, floppy diskettes, audiotapes, videotapes, or CD-ROMs) must be marked in a manner consistent with the paragraph above so persons possessing the documents and persons with access to the information in or on the documents are aware they contain OUO information. When space is limited, as on the frame of a 35-mm slide, the page marking is sufficient.

ATTACHMENT 3

DISCLOSURE AND CHANGE IN STATUS OF SUI

1. DISCLOSURE OF SUI PROPRIETARY INFORMATION OR OFFICIAL USE INFORMATION TO SOURCES OUTSIDE OF DOE

SUI shall only be disclosed to sources outside of DOE under the following circumstances:

a. In the case of disclosure to Federal employees, the disclosure is necessary for the employee to perform his or her official duties;

b. In the case of disclosure to NETL site support contractors, the disclosure is consistent with NETL's rights in or to the SUI, and the disclosure is necessary for the contractor to perform a duly authorized task under the contract; and

c. In the case of disclosures not covered by paragraphs a. and b., the disclosure is consistent with NETL's rights in or to the SUI and the disclosure is subject to the terms of a duly authorized confidentiality agreement with the party receiving the information.

Any proposed disclosure not addressed above must be approved in writing by the custodian's supervisor and the NETL Office of Chief Counsel.

The custodian shall maintain a record of all disclosures of SUI.

2. CHANGE OF STATUS OF SENSITIVE UNCLASSIFIED INFORMATION

It is recognized that circumstances may arise in that sensitive unclassified information may change status and simply become information that are available for public disclosure. If possible, the proprietary, OUO, and protected information markings are to be removed from the information before dissemination.

If this is not possible, the markings shall be crossed through with a single line and signed and dated by the NETL custodian.

ATTACHMENT 4

TRANSMISSION OF SENSITIVE UNCLASSIFIED INFORMATION

1. Documents marked as sensitive unclassified information (SUI) must:

   a. Be transmitted outside secure areas in sealed opaque envelopes or wrappers, single wrapped, providing no portion of the SUI matter is distinguishable outside the wrapping (the use of U.S. Postal Service First Class Mail is authorized).

   b. Be transmitted using encrypted e-mail or secure facsimile machines whenever possible. However, if such communication capabilities are not available, and transmission in opaque envelopes or wrappers described in a. above, is not a feasible alternative, the use of regular e-mail or facsimile machines is authorized for the transmission of SUI material to an authorized recipient. Such transmission should be preceded by a telephone call to the addressee, so that he/she can receive and control the material as soon as possible. It should be noted that SUI material should never be posted on an Internet website that is accessible to the general public or otherwise be transmitted or used in any manner that would effectively result in the material being placed in the public domain.