DOE M 471.3-1

Approved: 4-9-03
Sunset Review: 4-9-05
Expires: 4-9-07

MANUAL FOR IDENTIFYING AND PROTECTING OFFICIAL USE ONLY INFORMATION

U.S. DEPARTMENT OF ENERGY
Office of Security

DISTRIBUTION:
All Departmental Elements

INITIATED BY:
Security Policy Staff

MANUAL FOR IDENTIFYING AND PROTECTING OFFICIAL USE ONLY INFORMATION

1. PURPOSE. This Department of Energy (DOE) Manual provides detailed requirements to supplement DOE O 471.3, *Identifying and Protecting Official Use Only Information,* dated 4-9-03.

2. SUMMARY. This Manual comprises two chapters that provide direction for identifying, marking, and protecting Official Use Only (OUO) information. These chapters address mandatory procedures and management processes. Chapter I describes the requirements for identifying and marking OUO information; Chapter II addresses protecting OUO information. The Contractor Requirements Document (CRD), Attachment 1, sets forth requirements of this Manual that apply to site/facility management contractors.

3. REFERENCES.

   a. 10 CFR Part 1004, Freedom of Information.

   b. DOE O 241.1A, *Scientific and Technical Information*, dated 4-9-01.

   c. DOE O 471.3, *Identifying and Protecting Official Use Only Information,* dated 4-9-03.

   d. DOE G 471.3-1, *Guide to Identifying Official Use Only Information*, dated 4-9-03.

   e. DOE 3750.1, *Work Force Discipline,* dated 3-23-83.

4. CONTACT. Questions concerning this Manual should be addressed to Information Classification and Control Policy at 301-903-5454.

BY ORDER OF THE SECRETARY OF ENERGY:

KYLE E. McSLARROW
Deputy Secretary

CONTENTS

CHAPTER I

IDENTIFYING AND MARKING OFFICIAL USE ONLY INFORMATION

1. IDENTIFYING INFORMATION AS OFFICIAL USE ONLY. To be identified as OUO, information must be unclassified and meet both of the following criteria:

   a. Have the potential to damage governmental, commercial, or private interests if disseminated to persons who do not need the information to perform their jobs or other DOE-authorized activities. The possible consequences to such interests should be carefully considered in each case.

   b. Fall under at least one of eight Freedom of Information Act (FOIA**)** exemptions (exemptions 2 through 9; information falling under exemption 1 can never be OUO because it covers information classified by Executive order). These exemptions describe types of information whose unauthorized dissemination could damage governmental, commercial, or private interests (see DOE G 471.3-1, *Guide to Identifying Official Use Only Information,* dated 4-9-03, for a discussion of FOIA exemptions 2 through 9).

2. DETERMINING WHETHER A DOCUMENT CONTAINS OFFICIAL USE ONLY INFORMATION. An unclassified document that is originated within a DOE/NNSA office, produced by or for that office, or under the control of that office may contain OUO information. Any employee from an office with cognizance over such information may determine whether such a document contains OUO information. The process is as follows:

   a. The employee first considers whether the information has the potential to damage governmental, commercial, or private interests if disseminated to persons who do not need the information to perform their jobs or other DOE-authorized activities.

   b. If the information is considered to have the potential for such damage, then the employee consults guidance issued under paragraphs 5a(3), 5a(4), or 5b(2) of DOE O 471.3. If the specific information in question is identified as OUO information in such guidance, then the employee determines that the document contains OUO information.

   c. If the information is considered to have the potential for such damage, but no guidance issued under paragraphs 5a(3), 5a(4), or 5b(2) of DOE O 471.3 covers the specific information in question, then the employee considers whether the information falls under at least one of FOIA exemptions 2 through 9 (consult the DOE G 471.3-1 for assistance in determining whether any of the exemptions apply). If the employee believes that the information falls under one of the FOIA

exemptions, then the employee may determine that the document contains OUO information.

d. If the employee finds no basis for identifying the information as OUO in guidance issued under DOE O 471.3 and does not believe the information falls under one of the FOIA exemptions, then the employee must not mark the document as containing OUO information.

3. MARKING A DOCUMENT THAT CONTAINS OFFICIAL USE ONLY INFORMATION.

a. Front Marking. The front marking includes the applicable FOIA exemption number and related category name (i.e., Exemption 2 - Circumvention of Statute; Exemption 3 - Statutory Exemption; Exemption 4 - Commercial/Proprietary; Exemption 5 - Privileged Information; Exemption 6 - Personal Privacy; Exemption 7 - Law Enforcement; Exemption 8 - Financial Institutions; Exemption 9 - Wells) and the name and organization of the employee making the determination and identifies the guidance used if the determination was based on guidance. (NOTE: The guidance referred to here is guidance issued under paragraphs 5a(3), 5a(4), or 5b(2) of DOE O 471.3, not the DOE directives guide (DOE G 471.3-1).) The employee making the determination ensures that the following marking is placed on the front of each 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:_____
Guidance (if applicable)_____

b. Page Marking. The employee making the determination must ensure that the words "Official Use Only" (or "OUO" if space is limited) are placed on the bottom of each page or, if more convenient, on just those pages containing the OUO information.

c. Marking E-mail Messages. The first line of an e-mail message containing OUO information must contain the abbreviation "OUO" before the beginning of the text. If the message itself is not OUO but an attachment contains OUO information, the message must indicate that the attachment is OUO. The attachment must have all required OUO markings.

d. Marking Special Format Documents. Special format documents (e.g., photographs, viewgraphs, films, magnetic tapes, floppy diskettes, audiotapes,

videotapes, DVDs, or CD-ROMs) must be marked in a manner consistent with paragraphs 3a and 3b above so persons possessing the documents and persons with access to the information in or on the documents are aware that they contain OUO information. When space is limited, as on the frame of a 35-mm slide, the page marking is sufficient.

e. Marking Documents Maintained in Restricted Access Files. Documents that may contain OUO information that are maintained in files to which access is restricted (e.g., personnel office files) do not need to be reviewed and marked while in these files or when retrieved from the files for reference, inventory, or similar purposes as long as the documents will be returned to the files and are not accessible by individuals who are not authorized access to the OUO information. However, a document removed from these files and not to be returned (or a copy of such document) must be reviewed to determine whether it contains OUO information and, if appropriate, marked. (NOTE: Documents that are moved from one restricted access file location to another for storage purposes do not need to be reviewed.) Documents that are removed for criminal, civil, or administrative law enforcement or prosecution purposes need not be reviewed or marked where parallel controls to this order are in place.

f. Transmittal Document. A document that (1) transmits an attachment or enclosure marked as containing OUO information and (2) does not itself contain classified or controlled information must be marked on its front as follows to call attention to the presence of OUO information in the attachments or enclosures.

Document transmitted contains OUO information

g. Removal of Official Use Only Markings.

(1) Markings Applied Based on Guidance. OUO markings applied based on guidance may be removed by any employee when the guidance used to make the determination states that the information is no longer OUO. (For example, a topic may state that unclassified information that describes certain deficiencies at a site/facility/security area that have not been corrected is OUO. Once those deficiencies have been corrected, the OUO marking may be removed.)

(2) Markings Applied Based on Employee's Evaluation. OUO markings applied based on an employee's evaluation may be removed by (1) the employee who initially applied the marking, (2) the supervisor of the employee who initially applied the marking, or (3) a FOIA authorizing official who approves the release of the document in response to a request made under FOIA.

Whoever makes the determination to remove the markings ensures that the markings are crossed out or otherwise obliterated and places the following marking on the bottom of the front of the document:

DOES NOT CONTAIN
OFFICIAL USE ONLY INFORMATION

Name/Org.: _____ Date: _____

h. Relationship of Official Use Only Markings to Other Types of Control Markings.

(1) Unclassified Documents. The OUO front marking must be applied to any unclassified document that contains OUO information regardless of any other unclassified control marking [e.g., Unclassified Controlled Nuclear Information (UCNI)].

(2) Classified Documents. OUO front and page markings must not be applied to any classified document that also contains OUO information. However, if the classified document has been portion marked, the acronym "OUO" must be used to indicate those portions containing only OUO information.

i. Marking Documents Generated Before the Date of this Manual. Unclassified documents generated before the date of this Manual are not required to be reviewed to determine whether they contain OUO information unless they are to be publicly released. Any such previously generated document determined to contain OUO information after the date of this Manual must be marked as indicated in paragraph 3 above. Such determination may be made by anyone in the organization that currently has cognizance over the information in the document. In addition, for unclassified documents marked as containing OUO information before the date of this Manual, the markings are not required to be updated to conform with the marking requirements in this Manual.

j. Obsolete Markings. From July 18, 1949, to October 22, 1951, the Atomic Energy Commission used the term "Official Use Only" as a designation for certain classified information. Documents from this time period with an OUO marking must be handled as Confidential National Security Information pending a determination of their proper classification. Refer to DOE M 475.1-1A, *Identifying Classified Information,* dated 5-8-98 [National Nuclear Security Administration (NNSA) certified 2-26-01], for specific procedures.

CHAPTER II

PROTECTING OFFICIAL USE ONLY INFORMATION

1. ACCESS TO OFFICIAL USE ONLY INFORMATION. Access to (a) documents marked as containing OUO information and (b) OUO information from such documents must only be provided to those persons who require the information to perform their jobs or other DOE-authorized activities. The responsibility for determining whether someone has a valid need for such access rests with the person who has authorized possession, knowledge, or control of the information or document and not on the prospective recipient.

2. PHYSICAL PROTECTION REQUIREMENTS.

   a. Protection in Use. Reasonable precautions must be taken to prevent access to documents marked as containing OUO information by persons who do not require the information to perform their jobs or other DOE-authorized activities (e.g., don't read an OUO document in a public place, such as a cafeteria, on public transportation).

   b. Protection in Storage. Documents marked as containing OUO information may be stored in unlocked receptacles such as file cabinets, desks, or bookcases when Government or Government-contractor internal building security is provided during non-duty hours. When such internal building security is not provided, comparable measures should be taken, such as storing the documents in a locked room or other locked receptacle (e.g., a locked file cabinet, desk, bookcase, or briefcase).

   c. Reproduction. Documents marked as containing OUO information may be reproduced without the permission of the originator to the minimum extent necessary to carry out official activities. Copies must be marked and protected in the same manner as originals. Copy machine malfunctions must be cleared and all paper paths checked for papers containing OUO information. Excess paper containing OUO information must be destroyed as described below.

   d. Destruction. A document marked as containing OUO information must be destroyed by using a strip-cut shredder that produces strips no more than 1/4-inch wide or by any other means that provides a similar level of destruction that has been approved by the local security office. The decision to dispose of any DOE or NNSA document, whether it contains OUO information or not, must be consistent with the policies and procedures for records disposition.

e. Transmission.

(1) By Mail—Outside of a Facility.

(a) Use a sealed, opaque envelope or wrapping and mark the envelope or wrapping with the recipient's address, a return address, and the words "TO BE OPENED BY ADDRESSEE ONLY."

(b) Any of the following U.S. mail methods may be used: First Class, Express, Certified, or Registered Mail.

(c) Any commercial carrier may be used.

(2) By Mail—Within a Facility. Use a sealed, opaque envelope with the recipient's address and the words "TO BE OPENED BY ADDRESSEE ONLY" on the front.

(3) By Hand—Between Facilities or Within a Facility. A document marked as containing OUO information may be hand carried between or within a facility as long as the person carrying the document can control access to the document being transported.

(4) Over Telecommunications Circuits. Documents marked as containing OUO should be protected by encryption when transmitted over telecommunications circuits whenever possible. This may be accomplished through DOE public key systems or use of encryption algorithms that comply with all applicable Federal laws, regulations, and standards (e.g., Entrust) that address the protection of sensitive unclassified information (see Chapter 9 of DOE M 200.1-1, "Public Key Cryptography and Key Management"). However, if such encryption capabilities are not available and transmission by mail is not a feasible alternative, then regular e-mail or facsimile machines may be used to transmit the document.

(a) By Unencrypted Facsimile. An unencrypted facsimile transmission must be preceded by a telephone call to the recipient so that he or she can control the document when it is received.

(b) By E-mail without Encryption. If encryption is not available and some form of protection is desired, the OUO information may be included in a word processing file that is protected by a password and attached to the email message. Then the sender can call the recipient with the password so that he or she can access the file.

f. Transmission over Voice Circuits. OUO information transmitted over voice circuits should be protected by encryption (see DOE M 200.1-1, Chapter 9, for requirements) whenever possible. However, if such encryption capabilities are not available and transmission by other encrypted means is not a feasible alternative, then regular voice circuits may be used.

g. Processing on Automated Information Systems. An automated information system (AIS) or AIS network must provide methods (e.g., authentication, file access controls, passwords) to prevent access to OUO information stored on the system by persons who do not require the information to perform their jobs or other DOE-authorized activities.

CONTRACTOR REQUIREMENTS DOCUMENT

DOE M 471.3-1, MANUAL FOR IDENTIFYING AND PROTECTING OFFICIAL USE ONLY INFORMATION

Regardless of the performer of the work, the contractor is responsible for compliance with the requirements of this Contractor Requirements Document (CRD). The contractor is responsible for flowing down the requirements of this CRD to subcontracts at any tier to the extent necessary to ensure the contractor's compliance with the requirements. The contractor must:

1. Ensure that unclassified information meeting both of the following requirements is identified as OUO information.

    a. The information has the potential to damage governmental, commercial, or private interests if disseminated to persons who do not need the information to perform their jobs or other DOE-authorized activities. The possible consequences to such interests should be carefully considered in each case.

    b. The information falls under at least one of eight Freedom of Information Act (FOIA) exemptions (exemptions 2 through 9; information falling under exemption 1 can never be OUO because it covers information classified by Executive order). These exemptions describe types of information whose unauthorized dissemination could damage governmental, commercial, or private interests (see Chapter II of the DOE G 471.3-1, *Guide to Identifying Official Use Only Information,* dated 4-9-03, for a discussion of FOIA exemptions 2 through 9).

2. Ensure that unclassified documents originated by the contractor, produced by or for the contractor, or under the control of the contractor that have the potential to damage governmental, commercial, or private interests are identified as containing OUO information based on (a) guidance issued by the DOE, (b) guidance developed by the contractor that is consistent with guidance issued by the DOE, or (c) consideration that the information meets the criterion contained in paragraph 1b.

3. Ensure that a document containing OUO information is marked as follows:

    a. Front Marking. The front marking includes the applicable FOIA exemption number and related category name (i.e., Exemption 2 - Circumvention of Statute; Exemption 3 - Statutory Exemption; Exemption 4 - Commercial/Proprietary; Exemption 5 - Privileged Information; Exemption 6 - Personal Privacy; Exemption 7 - Law Enforcement; Exemption 8 - Financial Institutions; Exemption 9 - Wells), the name and organization of the employee making the determination, and identifies the guidance used if the determination was based on guidance. [NOTE: The guidance referred to here is guidance issued by the DOE,

not the DOE directives guide (DOE G 471.3-1).] This marking is placed on the front of each 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: _____
Guidance (if applicable) _____

b. Page Marking. The words "Official Use Only" (or "OUO" if space is limited) are placed on the bottom of each page or, if more convenient, on just those pages containing the OUO information.

c. Marking E-mail Messages. The first line of an e-mail message containing OUO information must contain the abbreviation "OUO" before the beginning of the text. If the message itself is not OUO but an attachment contains OUO information, the message must indicate that the attachment is OUO. The attachment must have all required OUO markings.

d. Marking Special Format Documents. Special format documents (e.g., photographs, viewgraphs, films, magnetic tapes, floppy diskettes, audiotapes, videotapes, DVDs, or CD-ROMs) must be marked in a manner consistent with paragraphs 3a and 3b above so persons possessing the documents and persons with access to the information in or on the documents are aware that they contain OUO information. When space is limited, as on the frame of a 35-mm slide, the page marking is sufficient.

e. Marking Documents Maintained in Restricted Access Files. Documents that may contain OUO information that are maintained in files to which access is restricted (e.g., personnel office files) do not need to be reviewed and marked while in these files or when retrieved from the files for reference, inventory, or similar purposes as long as the documents will be returned to the files and are not accessible by individuals who are not authorized access to the OUO information. However, a document removed from these files and not to be returned (or a copy of such document) must be reviewed to determine whether it contains OUO information and, if appropriate, marked. (NOTE: Documents that are moved from one restricted access file location to another for storage purposes do not need to be reviewed.) Documents that are removed for criminal, civil, or administrative law enforcement or prosecution purposes need not be reviewed or marked where parallel controls to this order are in place.

f. Transmittal Document. A document that (a) transmits an attachment or enclosure marked as containing OUO information and (b) does not itself contain classified

or controlled information must be marked on its front as follows to call attention to the presence of OUO information in the attachments or enclosures:

Document transmitted contains OUO information

4. Remove OUO markings from a document when it no longer warrants such protection. OUO markings applied based on guidance issued by DOE may be removed when the guidance used to make the determination states that the information is no longer OUO. (For example, a topic may state that unclassified information that describes certain deficiencies at a site/facility/security area that have not been corrected is OUO. Once those deficiencies have been corrected, the OUO marking may be removed.)

5. Comply with the following marking requirements for documents containing OUO information and other types of classified or controlled information:

   a. Unclassified Documents. The OUO front marking must be applied to any unclassified document that contains OUO information regardless of any other unclassified control marking [e.g., Unclassified Controlled Nuclear Information (UCNI)].

   b. Classified Documents. OUO markings must not be applied to any classified document that also contains OUO information. However, if the classified document has been portion marked, the acronym "OUO" must be used to indicate those portions containing only OUO information.

6. Not require unclassified documents generated before the date of this CRD to be reviewed to determine whether they contain OUO information unless they are to be publicly released. Any such previously generated document determined to contain OUO information after the date of this CRD must be marked as indicated in paragraph 3 above. Such determination may be made by anyone with cognizance over the information in the document. In addition, for unclassified documents marked as containing OUO information before the date of this CRD, the markings are not required to be updated to conform with the marking requirements in this CRD.

7. Be cognizant of the fact that from July 18, 1949, to October 22, 1951, the Atomic Energy Commission used the term "Official Use Only" as a designation for certain classified information. Documents from this time period with an OUO marking must be handled as Confidential National Security Information pending a determination of their proper classification. (See Chapter V, Part B, paragraph 8d, of the CRD for DOE M 475.1-1A, *Identifying Classified Information,* dated 5-8-98 [National Nuclear Security Administration (NNSA) certified 2-26-01], for specific procedures.

8. Ensure that access to (a) documents marked as containing OUO information or (b) OUO information from such documents is provided only to those persons who need to know the information to perform their jobs or other DOE-authorized activities.

9. Ensure that the following protection requirements are followed:

   a. Protection in Use. Reasonable precautions must be taken to prevent access to documents marked as containing OUO information by persons who do not require the information to perform their jobs or other DOE-authorized activities (e.g., don't read an OUO document in a public place, such as a cafeteria, on public transportation, etc.).

   b. Protection in Storage. Documents marked as containing OUO information may be stored in unlocked receptacles such as file cabinets, desks, or bookcases when Government or Government-contractor internal building security is provided during nonduty hours. When such internal building security is not provided, comparable measures should be taken, such as storing the documents in a locked room or other locked receptacle (e.g., a locked file cabinet, desk, bookcase, or briefcase).

   c. Reproduction. Documents marked as containing OUO information may be reproduced without the permission of the originator to the minimum extent necessary to carry out official activities. Copies must be marked and protected in the same manner as originals. Copy machine malfunctions must be cleared and all paper paths checked for papers containing OUO information. Excess paper containing OUO information must be destroyed as described below.

   d. Destruction. A document marked as containing OUO information must be destroyed by using a strip-cut shredder that produces strips no more than 1/4-inch wide or by any other means that provides a similar level of destruction that has been approved by the local security office. The decision to dispose of any DOE or NNSA document, whether it contains OUO information or not, must be consistent with the policies and procedures for records disposition.

   e. Transmission.

      (1) By Mail—Outside of a Facility.

         (a) Use a sealed, opaque envelope or wrapping and mark the envelope or wrapping with the recipient's address, a return address, and the words "TO BE OPENED BY ADDRESSEE ONLY."

         (b) Any of the following U.S. mail methods may be used: First Class, Express, Certified, or Registered Mail.

         (c) Any commercial carrier may be used.

(2) By Mail—Within a Facility. Use a sealed, opaque envelope with the recipient's address and the words "TO BE OPENED BY ADDRESSEE ONLY" on the front.

(3) By Hand—Between Facilities or Within a Facility. A document marked as containing OUO information may be hand carried between or within a facility as long as the person carrying the document can control access to the document being transported.

(4) Over Telecommunications Circuits. Documents marked as containing OUO should be protected by encryption when transmitted over telecommunications circuits whenever possible. This may be accomplished through DOE public key systems or use of encryption algorithms that comply with all applicable Federal laws, regulations, and standards (e.g., Entrust) that address the protection of sensitive unclassified information (see Chapter 9 of DOE M 200.1-1, "Public Key Cryptography and Key Management"). However, if such encryption capabilities are not available and transmission by mail is not a feasible alternative, then regular e-mail or facsimile machines may be used to transmit the document.

(a) By Unencrypted Facsimile. An unencrypted facsimile transmission must be preceded by a telephone call to the recipient so that he or she can control the document when it is received.

(b) By E-mail without Encryption. If encryption is not available and some form of protection is desired, the OUO information may be included in a word processing file that is protected by a password and attached to the email message. Then the sender can call the recipient with the password so that he or she can access the file.

f. Transmission over Voice Circuits. OUO information transmitted over voice circuits should be protected by encryption (see DOE M 200.1-1, Chapter 9, for requirements) whenever possible. However, if such encryption capabilities are not available and transmission by other encrypted means is not a feasible alternative, then regular voice circuits may be used.

g. Processing on Automated Information Systems. An automated information system (AIS) or AIS network must provide methods (e.g., authentication, file access controls, passwords) to prevent access to OUO information stored on the system by persons who do not require the information to perform their jobs or other DOE-authorized activities.