Department of Energy

Bonneville Power Administration
P.O. Box 3621
Portland, Oregon 97208-3621

GENERAL COUNSEL

June 10, 2005

In reply refer to: LC-7

4/12/05
70FR19125
(4)

RECEIVED
2005 JUN 14 AM 11:13
RULES AND DIRECTIVES
BRANCH
USNRC

VIA EXPRESS MAIL

Chief, Rules and Directives Branch
Division of Administrative Services
Office of Administration
U.S. Nuclear Regulatory Commission
Mail Stop T6-D59
Washington, D.C. 20555-0001

VIA FEDERAL EXPRESS

Nuclear Regulatory Commission Headquarters
11545 Rockville Pike – Room T-6D59
Rockville, Maryland 20852-2747

Re: 70 Federal Register 19,125 (April 12, 2005) Nuclear Regulatory Commission "Proposed Generic Communication: Grid Reliability and the Impact on Plant Risk and the Operability of Offsite Power" - Comments of the Bonneville Power Administration ("BPA")

Dear Sirs and Madames:

Enclosed please find an original and four copies of the "Comments of the Bonneville Power Administration" in response to the above-referenced Federal Register Notice "Notice of opportunity for public comment." Also enclosed, and being routed to each of the two addressees indicated above, is a stamped, self-addressed return envelope together with a fifth copy of the "Comments of the Bonneville Power Administration."

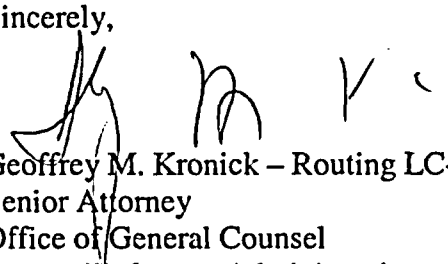
E-RIDS=ADM-03

Cdd = A. Markley (AWM)
Jose Calvo (JAC7)
J.E. Lamb (CJEL1)

SISP Review Complete
Template=ADM-013

Upon receipt of the respective sets of comments being routed to each of the two addressees, if you could please date stamp the "fifth copy" of the BPA Comments being submitted, and return that copy to me in the stamped, self-addressed envelope enclosed. Thank you for your assistance in this matter.

Sincerely,



Geoffrey M. Kronick – Routing LC-7
Senior Attorney
Office of General Counsel
Bonneville Power Administration
(503) 230-4201
Facsmile (503) 230-7405
E-mail – gmkronick@bpa.gov

cc: w/one copy of Comments of BPA
Pamela R. Bradley, Esq.
Mail Drop – PE-13
Energy Northwest
P O Box 968
Richland, WA 99352-0968

Comments of the Bonneville Power Administration

Introduction

The Bonneville Power Administration ("BPA"), a self-financing Federal power marketing administration within the U.S. Department of Energy ("DOE") respectfully submits the following comments in response to the Federal Register notice and opportunity for public comment published by the U.S. Nuclear Regulatory Commission on April 12, 2005 at 70 Fed. Reg. 19,125. That notice concerns a "Proposed Generic Communication: Grid Reliability and the Impact on Plant Risk and the Operability of Offsite Power" in the form of a generic letter to be routed to all holders of operating licenses for nuclear power reactors, save those who have permanently ceased operations and have certified that fuel has been permanently removed from the reactor vessel.

Background

BPA's primary enabling legislation includes the following federal statutes: the Bonneville Project Act of 1937 (the "Project Act"); the Flood Control Act of 1944 (the "Flood Control Act"); Public Law 88-552 (the "Regional Preference Act"); the Federal Columbia River Transmission System Act of 1974 (the "Transmission System Act"); and the Northwest Electric Power Planning and Conservation Act of 1980 (the "Northwest Power Act"). BPA markets electric power from 30 federal hydroelectric projects, most of which are located in the Columbia River Basin and all of which are owned and operated either by the United States Army Corps of Engineers ("Corps") or the United States Bureau of Reclamation ("Bureau"). These projects have an expected aggregate output of roughly 9,000 average megawatts under median water conditions. Bonneville also has acquired and markets power from several non-federally owned and operated projects, including the Columbia Generating Station, an operating nuclear generating station owned by Energy Northwest, located on the Hanford Nuclear Reservation near Richland, Washington, and having a rated capacity of approximately 1150 megawatts.

Bonneville also has constructed and operates and maintains a high voltage transmission system comprising approximately 75% of the bulk transmission capacity in the Pacific Northwest Region of the United States. Bonneville uses this transmission capacity to deliver power to its customers and makes transmission capacity available to other utilities and power marketers. For purposes of these instant "comments" being submitted to the NRC, it should be understood that BPA provides station service to the Columbia Generating Station owned and operated by Energy Northwest, a resource for which BPA is the only customer, purchasing all output of this nuclear generating station and paying all of its costs through a 1970 operating agreement between BPA and Energy Northwest; an arrangement that also involves a complex set of three-way contracts (termed "Net-Billing Agreements") between Energy Northwest, over 114 public utility districts and municipalities in the Pacific Northwest who are also BPA customers, and BPA.

Post 9-11 Security Protocols

As NRC is aware, following the terrorist attack on September 11, 2001, and the subsequent passage of the U.S.A. Patriot Act, many government departments initiated new protocols for the handling of information that could possibly be of use to terrorists in planning and/or implementing terrorist acts against the United States. DOE promulgated precisely such a new protocol in the form of DOE Order 471.3, "Identifying and Protecting Official Use Only Information," April 9, 2003 ("DOE Order"). Further guidance was afforded by a contemporaneous "Manual for Identifying and Protecting Official Use Only Information," DOE M 471.3-1 ("DOE Manual"), and a "Guide to Identifying Official Use Only Information," DOE G 471.3-1.[1] The DOE Order 471.3 and the "DOE Manual" are appended here as Appendix 1 and Appendix 2, respectively.

In adapting these "protocols," which DOE O 471.3 makes applicable to BPA as indeed in the case of all departmental elements within DOE, [2] BPA had set forth these requirements in its own internal Procedures contained in the BPA Manual, Chapter 1081: "Dissemination of Critical and Sensitive Information, Including Information Pertaining to Critical Infrastructure,"08/15/03. A copy of Chapter 1081 of the BPA Manual is appended here as Appendix 3.

Definition of Critical Infrastructure Information

Section 1081.2 (at page 2) ("Definitions") of Chapter 1081 of the BPA Manual defines "Critical Infrastructure Information" ("CII") as:

For the energy component of the national economy, this means information about proposed or existing critical infrastructure which (i) relates to the production, generation, transportation, transmission, or distribution of energy, and (ii) might substantially increase the effectiveness of persons who would intend impair or disable such infrastructure. Examples of material which may contain CII include power flow studies, the maps of important transmission lines, inspection reports, detailed layouts of facilities such as substations, powerhouses, switchyards, emergency action plans, FERC Form No. 715 (Annual Transmission Plan and Evaluation Report), generation or transmission system scheduled outage information, telecommunications diagrams, and descriptions of supporting systems such as water supply, transportation access and hazardous waste handling system.

(Emphasis added.) [3]

This definition would encompass the types of information that NRC proposes, in its April 12, 2005, Federal Register Notice, to obtain from NRC licensees, in this case Energy

[1] "The "Guide" is not "measurement sensitive," and describes only suggested non-mandatory approaches for meeting requirements.

[2] See Appendix 1 at Page 1, Item 3 (a) (Applicability) and also at Attachment 1, page 1, of Appendix

[3] This specific definition contained in BPA Manual Chapter 1081 is obtained form the Critical Infrastructure Information Act of 2001.

Northwest. NRC's Federal Register notice specifies that the "generic letter" to be issued "will obtain information form its licensees" in four areas:

(1) Use of nuclear power plant/transmission system operator protocols and real time contingency analysis programs to monitor grid conditions to determine operability of offsite power systems under plant technical specifications

(2) Use of nuclear power plant/transmission system operator protocols and real time contingency analysis programs to monitor grid conditions for consideration in maintenance risk assessments

(3) Offsite power restoration procedures in accordance with Section 2 of Regulatory Guide 1.155, "Station Blackout,"

(4) Losses of offsite power caused by grid failures at a frequency of $\geq$ 20 Years in accordance with Regulatory Guide 1.155.

Compliance with DOE Order 471.3 and Protection of Critical Infrastructure Information

Given the close working relationship between Energy Northwest (formerly the Washington Public Power Supply System) and BPA, BPA staff have already discussed the anticipated need of Energy Northwest for various items of transmission-related information that is also Critical Infrastructure Information (or "CII") subject to DOE Order 471.3. In order to address both the need for Energy Northwest to obtain such Critical Infrastructure Information for its own purposes (i.e. provide information in response to NRC's proposed and imminent "generic letter"), and also provide the required "protection" from non-disclosure to third parties envisioned by DOE Order 471.3, BPA has prepared and discussed a "draft" Non-Disclosure Agreement with Energy Northwest legal counsel that would apply to such items of CII "transmission-related" data that BPA would provide to Energy Northwest.

This "draft" Non-Disclosure Agreement provides explicit agreements and safeguards against disclosure in the case where a third party, for example under the Washington State Public Disclosure Law, might seek this CII from Energy Northwest. Notably, however, Energy Northwest has indicated that it cannot, given its licensee relationship, agree to withhold any CII from NRC should it be so requested. BPA understands the significance and primacy of this need, but remains concerned with the primacy of its own security procedures that follow from DOE Order 471.3.

Anticipating the upcoming generic letter that is the subject of NRC's instant Federal Register notice and opportunity for comment, BPA has examined what appear to be the two source documents under which NRC provides guidance regarding non-disclosure of information. These sources are contained at 10 CFR § 2.390 (2005) and in the NRC's ("hereafter "Commission's") Policy Issuance in SECY-2004-0191; "Withholding Sensitive Unclassified Information Concerning Nuclear Power Reactors from Public Disclosure." BPA's concern is, of course, that the information that will be requested of Energy Northwest, NRC's licensee, once provided to NRC, will potentially be subject to

disclosure by NRC. Such disclosure, as previously indicated, would apparently conflict with BPA's security procedures.

10 CFR § 2.390

The categories of documents enumerated in 10 CFR § 2.390 includes, but is not limited to, "correspondence to and from the NRC regarding the issuance, denial, amendment, transfer, renewal, modification, suspension, revocation, or violation of a license, permit, or order, or regarding a rulemaking proceeding." It provides that the Commission may undertake a "balancing test" in order to determine if the "interests of the . . . agency urging nondisclosure and the public interest in disclosure" provides a "compelling reason for non-disclosure." 10 CFR § 2.390 (a).

SECY-04-0191

Similarly, SECY-04-0191, at Attachment 1, provides that there "may be information that could reasonably be expected to be useful to a potential adversary that does not meet the requirements established for designating the information as SGI [Safeguards information.] Again, SECY-04-0191 (Attachment 1) appears to set forth a similar evaluative process under which the Commission would determine what information "'could reasonably be expected to be useful to potential adversary's ability to plan or execute an attack or other malevolent act and the ability of a licensee or government agency to respond to such an attack." SECY-04-0191, Attachment 1 at page 1.

Conclusion

BPA thus respectfully urges the Commission to determine that any CII that would be provided to Energy Northwest by BPA, and subsequently to the Commission as a result of the generic letter proposed in this instant Federal Register notice, be determined by the Commission to be of the type of Non-Safeguards Sensitive Unclassified information that would not be subject to disclosure to any third parties. To this end, BPA would be willing to comply with such processes as the Commission may determine, that were not inconsistent with BPA/DOE security protocols, for providing such CII to the Commission prior to furnishing such information to Energy Northwest, in order to determine that such CII would not be subject to third party release.

Respectfully submitted,

Geoffrey M. Kronick
Senior Attorney
Of Attorneys for the Bonneville Power Administration
P. O. Box 3621, Routing LC-7
Portland, OR 97208-3621
(503) 230-4201

U.S. Department of Energy
Washington, D.C.

ORDER

DOE O 471.3

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

SUBJECT: IDENTIFYING AND PROTECTING OFFICIAL USE ONLY INFORMATION

1. OBJECTIVE. To establish a program within the Department of Energy (DOE), including the National Nuclear Security Administration (NNSA), to identify certain unclassified controlled information as Official Use Only (OUO) and to identify, mark, and protect documents containing such information. This information may be exempt from public release under the Freedom of Information Act (FOIA) and has the potential to damage governmental, commercial, or private interests if disseminated to persons who do not need to know the information to perform their jobs or other DOE-authorized activities.

2. CANCELLATION. None.

3. APPLICABILITY.

   a. DOE Elements. Except as noted in paragraph 3c, this Order applies to all DOE elements, including NNSA, listed on Attachment 1 that (1) identify information under their cognizance as OUO and mark documents they generate accordingly or (2) possess documents that are marked as containing OUO information or with equivalent markings from other agencies (see definitions for examples of such markings).

   b. Contractors.

      (1) The Contractor Requirements Document (CRD), Attachment 2, sets forth requirements of this Order that apply to contractors responsible for the management and operation of the Department-owned facilities (hereafter referred to as site/facility management contractors) whose contracts include the CRD.

      (2) This CRD must be included in site/facility management contracts that involve activities where OUO information and documents will be handled, used, or generated.

      (3) The officials identified in paragraph 5, Responsibilities, are responsible for notifying the contracting officers which site/facility management contracts are affected. Once notified, the contracting officer is responsible for incorporating the CRD into each affected site/facility management contract via the Laws, Regulations, and Departmental Directives clause of the contract.

(4) As the Laws, Regulations, and Departmental Directives clause of a site/facility management contract states, regardless of the performer of the work, the site/facility management contractor with the CRD incorporated into its contract is responsible for compliance with the requirements of the CRD. An affected site/facility management contractor is responsible for flowing down the requirements of this CRD to subcontracts at any tier to the extent necessary to ensure the site/facility management contractors' compliance with the requirements.

c. Exclusions. Consistent with the responsibilities identified in Executive Order 12344, the Director of the Naval Nuclear Propulsion Program will determine the applicability of this Order for activities and facilities under his control.

4. REQUIREMENTS.

a. To be identified as OUO, information must be unclassified; have the potential to damage governmental, commercial, or private interests if disseminated to persons who do not need to know the information to perform their jobs or other DOE-authorized activities; and 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). (See DOE M 471.3-1, *Manual for Identifying and Protecting Official Use Only Information,* dated 4-9-03, for additional details.)

b. An unclassified document originated within a program element must be evaluated to determine whether it contains OUO information. An unclassified document that is produced by or for DOE/NNSA or is under the control of DOE/NNSA may be evaluated to determine whether it contains OUO information. (NOTE: Documents maintained in restricted access files do not need to be reviewed 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. See DOE M 471.3-1, Chapter 1, for additional details.)

c. A document determined to contain OUO information must be marked as described in DOE M 471.3-1. (NOTE: Documents maintained in restricted access files do not need to be 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. See DOE M 471.3-1, Chapter I, paragraph 4e.)

d. A document determined to no longer warrant protection as OUO must have its markings removed as described in DOE M 471.3-1.

e. Access to (1) documents marked as containing OUO information or (2) OUO information from such documents must only be provided to those persons who need to know the information to perform their jobs or other DOE-authorized activities.

f. Documents marked as containing OUO information and other-Agency documents with equivalent markings must be protected as described in DOE M 471.3-1.

g. An administrative penalty as prescribed in DOE 3750.1, *Work Force Discipline*, dated 3-23-83, is imposed if an employee (1) intentionally releases OUO information from a document marked as containing OUO information to a person who does not need to know the information to perform his or her job or other DOE-authorized activities, (2) intentionally or negligently releases a document marked as containing OUO information to a person who does not need to know the information to perform his or her job or other DOE-authorized activities, (3) intentionally does not mark a document that is known to contain OUO information, or (4) intentionally marks a document that is known not to contain OUO information.

h. If a document marked as containing OUO information is requested under FOIA, the document is not automatically exempt from public release, but must be reviewed and processed under 10 CFR Part 1004.

i. Except for Unclassified Controlled Nuclear Information, which is identified, marked, and protected under DOE O 471.1A, *Identification and Protection of Unclassified Controlled Nuclear Information,* dated 6-30-00, and DOE M 471.1-1, *Identification and Protection of Unclassified Controlled Nuclear Information Manual,* dated 6-30-00, and Naval Nuclear Propulsion Information, which is controlled under 32 CFR Part 250, OUO markings are the only markings to be used within DOE to designate documents containing unclassified controlled information. Additional markings that are based on law, regulation, or other DOE directives that convey additional advice on handling or access restrictions (e.g., "Source Selection Information—See FAR 2-101and 3.104"; "Protected CRADA Information"; "Export Controlled Information") are allowed.

5. RESPONSIBILITIES.

a. Secretarial Officers.

(1) Review procurement requests for new site/facility management contracts and, if appropriate, ensure that the requirements of the CRD of this directive are included in the contracts.

(2) Ensure that requirements contained in paragraph 4 of this Order are implemented by employees within their respective organizations.

(3) May develop and approve guidance to be used by all employees to identify documents containing OUO information under their cognizance and forward such guidance to the Director, Office of Security, for issuance.

(4) May develop, approve, and issue guidance to be used only by employees within their respective organizations to identify documents containing OUO information. Such guidance must be consistent with guidance issued under paragraphs 5a(3) and 5b(2).

b. Director, Office of Security.

(1) Develops and issues policies and procedures to identify OUO information and to identify and mark documents containing such information.

(2) Develops and issues guidance, with the concurrence of the program office with cognizance over the information, to assist individuals in determining whether a document contains OUO information. Issues guidance for use by all DOE employees that was developed and approved by Secretarial officers under paragraph 5a(3).

(3) Develops and issues protection requirements for OUO information.

(4) Develops and disseminates training material and conducts training sessions to assist individuals in identifying documents containing OUO information and marking such documents.

c. Freedom of Information Officers. Coordinate requests for documents under FOIA.

d. Contracting Officers.

(1) After notification by the appropriate program official, incorporate the CRD into the affected site/facility management contract in accordance with the Laws, Regulations, and DOE Directives clause of the contracts.

(2) Assist originators of procurement requests who want to incorporate the requirements of the CRD of this Order in new non site/facility management contracts, as appropriate.

6. DEVIATIONS FROM REQUIREMENTS. A Secretarial Officer may propose a variance (i.e., an alternate or equivalent means of meeting a requirement) or request a waiver from a specific requirement in this Order or in DOE M 471.3-1. This proposal must (a) identify the Order or Manual requirement for which a variance or waiver is being requested; (b) explain why a variance or waiver is needed; and (c) if requesting a variance, describe the alternate or equivalent means for meeting the requirement. The

proposal must be submitted to the Director, Office of Security, for approval. The Director's decision must be made within 30 days. The Office of Security will review each approved variance or waiver periodically to ensure it is still needed.

7. REFERENCES.

a. 10 CFR Part 1004, Freedom of Information.

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

c. DOE M 471.3-1, *Manual for 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.

8. DEFINITIONS.

a. Document. Recorded information regardless of its medium or characteristics.

b. Equivalent markings. Other-Agency information control markings that are equivalent to DOE Official Use Only (OUO) include but are not limited to the following: "For Official Use Only" (FOUO) from the Department of Defense and many other agencies, "Sensitive But Unclassified" (SBU) from the Department of State, and "Limited Official Use" (LOU) from the Department of Justice.

c. Information. Facts, data, or knowledge itself regardless of the medium of its conveyance. (Documents are deemed to convey or contain information and are not considered to be information per se.)

d. Official Use Only (OUO) information. Certain unclassified information that may be exempt from public release under the Freedom of Information Act and has the potential to damage governmental, commercial, or private interests if disseminated to persons who do not need to know the information to perform their jobs or other DOE authorized activities.

9. CONTACT. Questions concerning this Order 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

DEPARTMENT OF ENERGY ORGANIZATIONS TO WHICH DOE O 471.3,
***Identifying and Protecting Official Use Only Information*, IS APPLICABLE**

Office of the Secretary
Office of the Chief Information Officer
Office of Civilian Radioactive Waste Management
Office of Congressional and Intergovernmental Affairs
Office of Counterintelligence
Departmental Representative to the Defense Nuclear Facilities Safety Board
Office of Economic Impact and Diversity
Office of Energy Efficiency and Renewable Energy
Energy Information Administration
Office of Environment, Safety and Health
Office of Environmental Management
Office of Fossil Energy
Office of General Counsel
Office of Hearings and Appeals
Office of Independent Oversight and Performance Assurance
Office of the Inspector General
Office of Intelligence
Office of Management, Budget and Evaluation and Chief Financial Officer
National Nuclear Security Administration
Office of Nuclear Energy, Science and Technology
Office of Policy and International Affairs
Office of Public Affairs
Office of Science
Secretary of Energy Advisory Board
Office of Security
Office of Worker and Community Transition
Office of Energy Assurance
Bonneville Power Administration
Southeastern Power Administration
Southwestern Power Administration
Western Area Power Administration

CONTRACTOR REQUIREMENTS DOCUMENT
DOE O 471.3, *Identifying 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 shall:

1. Determine whether unclassified documents created and/or handled in the performance of this contract contain Official Use Only (OUO) information. (See Chapter I, paragraphs 2a and 2b, of the CRD for DOE M 471.3-1, *Manual for Identifying and Protecting Official Use Only Information*, dated 4-9-03.)

2. Ensure that documents determined to contain OUO information are marked appropriately. (See Chapter I, paragraph 4, of the CRD for DOE M 471.3-1.) Except for Unclassified Controlled Nuclear Information (UCNI) and Naval Nuclear Propulsion Information (NNPI), OUO markings are the only markings to be used to designate documents containing unclassified controlled information. Additional markings that are based on law, regulation, or other DOE CRD that convey additional advice on handling or access restrictions (e.g., "Protected CRADA Information," "Export Controlled Information") are allowed.

3. Ensure that documents determined to no longer warrant protection as OUO have their markings removed. [See Chapter I, paragraphs 4g(1) and 4g(2) of the CRD for DOE M 471.3-1.]

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

5. Ensure that documents marked as containing OUO information and other-Agency documents with equivalent markings [e.g., "For Official Use Only" (FOUO) from the Department of Defense; "Sensitive But Unclassified" (SBU) from the Department of State; "Limited Official Use" (LOU) from the Department of Justice] are protected. (See Chapter II, paragraph 2, of the CRD for DOE M 471.3-1.)

6. Ensure that a request for a variance (i.e., an alternate or equivalent means of meeting a requirement) or waiver from any requirements in the CRD for DOE O 471.3 or DOE M 471.3-1 are provided to the appropriate Secretarial Officer. Such request must (a) identify the requirement for which a variance or waiver is being requested; (b) explain why the variance or waiver is needed; and (c) if requesting a variance, describe the alternate or equivalent means for meeting the requirement.

7. Impose an administrative penalty, as appropriate, if (a) OUO information from a document marked as containing OUO information is intentionally released to a person who does not need to know the information to perform his or her job or other DOE-authorized activities, (b) a document marked as containing OUO information is intentionally or negligently released to a person who does not need to know the information to perform his or her job or other DOE-authorized activities, (c) a document that is known to contain OUO information is intentionally not marked, or (d) a document that is known to not contain OUO information is intentionally marked as containing such information.

Appendix 2

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.

1081.1 PURPOSE

To establish policies and define roles and responsibilities for dissemination of critical and sensitive information, including such information pertaining to critical infrastructure. The information can be disseminated by way of hard copy, electronic form, external web page, and/or verbally. Such information can be in any of the following classifications: Unclassified, For Official Use Only, Proprietary, Critical/Sensitive for National Critical Infrastructure.

For the purposes of this chapter, critical and sensitive information, including that pertaining to critical infrastructure, is to be protected to the extent possible from misuse, by others outside of BPA, which could contribute to disruption of the operation of such infrastructure. The policy of the United States is that any physical or virtual disruption of the operation of the critical infrastructure of the United States should be rare, brief, geographically limited in effect, manageable, and minimally detrimental to the economy, human and government services, and national security of the United States. This chapter contains BPA's policy regarding the dissemination of information pertaining to critical and sensitive information, with special emphasis on critical infrastructure information.

1081.2 DEFINITIONS

A. **Confidentiality Agreement:** An agreement between BPA and another person or entity who requires access to critical and sensitive information. Under the agreement, the person or entity receives the critical and sensitive information only on a need-to-know basis, and gives their explicit assurance that the information that they receive will not be copied, shared with another party, or released or distributed without BPA's prior authorization. Normally, Confidentiality Agreements are signed to ensure that the receiving party has read and understands the conditions of the agreement.

B. **Critical and Sensitive Information (CSI):** Information which must be safeguarded from loss, misuse, compromise, unauthorized access, or modification, because such actions may adversely affect the business, security or other interests of the government, or the privacy of individuals; or which may otherwise be used by BPA's competitors or adversaries (including, but not limited to, other utilities, contractors, foreign interests, or disgruntled employees) to harm or embarrass BPA, or to gain an unfair advantage. Examples of Critical and Sensitive Information include confidential legal strategies, employee personnel files, contract negotiations, pricing and business strategies, active investigations, critical infrastructure vulnerabilities, etc. Critical and Sensitive Information can exist in the form of printed documents, electronically stored information, telecommunications traffic, or the spoken word.

C. **Critical and Sensitive Information List (CSIL):** A list that identifies aspects of a program or functions, whether classified or unclassified, requiring safeguarding under BPA's OPSEC Plan (revised April 2002).

D. **Critical Infrastructure:** Systems and assets, whether physical or virtual, so vital to the United States that the impaired capacity, incapacity or destruction of them would have a debilitating impact on the security, economy, or public health or safety of the Nation or the Pacific Northwest region.

E. **Critical Infrastructure Information (CII):** For the energy component of the national economy, this means information about proposed or existing critical infrastructure which (i) relates to the production, generation, transportation, transmission, or distribution of energy, and (ii) might substantially increase the effectiveness of persons who would intend impair or disable such infrastructure. Examples of material which may contain CII include power flow studies, the maps of important transmission lines,

inspection reports, detailed layouts of facilities such as substations, powerhouses, switchyards, emergency action plans, FERC Form No. 715 (Annual Transmission Plan and Evaluation Report), generation or transmission system scheduled outage information, telecommunications diagrams, and descriptions of supporting systems such as water supply, transportation access and hazardous waste handling system.

F. **Custodial Organization:** The BPA organization or work group that has control of and custodial responsibility for certain CII.

G. **Cyber Security:** The cyber security protection procedures described in the BPA Cyber Security Protection Plan and associated policies.

H. **Maps:** Drawings, plans, diagrams, etc. Examples include drawings of substations, transmission line or tower locations, power plant and hydro facility layouts, hazardous waste locations, public water supply sources, specific gas pipeline locations, telecommunications system diagrams, or sensitive transportation sector diagrams (such as a hazardous waste transportation route).

I. **National Environmental Policy Act (NEPA) Documents:** National Environmental Policy Act of 1969; NEPA documents include environmental impact statements (EISs), environmental assessments (EAs), supplemental analyses (SAs), records of decision (RODs), categorical exclusions (CXs), documents prepared in support of NEPA document preparation, and other documents related to the fulfillment of the requirements of this Act.

J. **Need To Know:** Legitimate requirement of a person or organization to know, access, or possess CSI in performance of official job duties; a determination made by an authorized holder of CSI that a prospective recipient requires access to specific CSI information in order to perform official function.

K. **Official Use Only (OUO):** Certain unclassified information that should be protected because of sensitive governmental, commercial, or private interests. Required to fall within one of the nine FOIA exemptions designed to protect all sensitive government information, classified and unclassified, from public release.

L. **Operations Security Program (OPSEC):** A program designed to disrupt or defeat the ability of foreign intelligence or other adversaries to exploit sensitive BPA activities or information and to prevent the unauthorized disclosure of such information.

M. **OPSEC Working Group:** A formally designated cross-agency group, comprised of representatives of custodial organizations, that provides OPSEC advice to Management as described in 1080.4(E) of BPA Manual Chapter 1080 – Operations Security.

N. **Terrorism:** The calculated use of violence or threat of violence to intimidate or disrupt governments or societies in pursuit of goals that are generally political, religious, or ideological. As defined in 18 U.S.C. § 2332b(g)(5), actions which include the destruction of an energy facility, sabotage of a nuclear facility, murder of a federal employee, destruction of an interstate gas pipeline, etc.

1081.3 POLICY

BPA's policy is to protect critical and sensitive information, including such information pertaining to critical infrastructure. Critical and Sensitive Information Lists (CSIL) are incorporated into the BPA OPSEC Plan to describe information that should be identified as critical and sensitive. This policy protects critical and sensitive information, including information pertaining to critical infrastructure, from unauthorized use, compromise or disclosure.

1081.4 RESPONSIBILITIES

A. **All Employees and contractors** have a primary responsibility for compliance with BPAM 1080 and 1081 and adherence to OPSEC practices and safeguards issued pursuant to this chapter. Employees and contractors are responsible for protecting CSI; notifying the workgroup Vice President or OPSEC Program Manager when CSI is discovered on an external BPA web page(s) or when any other inappropriate CSI release is discovered.

B. **Manager for Security and Emergency Management**, directly or through the OPSEC Program Manager, is responsible for: (1) assisting in the oversight of external web content in conjunction with the web content managers/Web Masters; (2) periodically assessing the effectiveness and compliance with this chapter in conjunction with affected Custodial Organizations; (3) developing, with the advice of the OPSEC Working Group and the Office of General Counsel, any policies, safeguards, practices, or procedures necessary for compliance with agency directives and DOE OPSEC; and (4) assisting Custodial Organizations in the implementation of this chapter.

C. **Chief Information Officer (CIO)** is responsible to BPA's Administrator to develop, implement, and monitor Policy and Standard's for BPA's Information Technology infrastructure and to manage the cyber security program and initiatives; delegates certain authorities of the BPA Cyber Security Protection Plan.

D. **Chief Information Security Officer (CISO)** is an agent of the CIO; has responsibility and authority over the creation, modification, and implementation of the BPA Cyber Security Protection Plan; responsible for managing disclosure of information which might compromise BPA's cyber security infrastructure or critical/sensitive data; during a security emergency, assumes decision authority over all cyber security issues; available to assist workgroup Vice Presidents on cyber security issues.

E. **Web Designers/Web Masters/Content Authors** are responsible for understanding and applying this chapter while designing, modifying or adding to BPA web pages, especially external BPA web pages, or sharing information with external sources.

F. **OPSEC Program Manager** is responsible for chairing the quarterly OPSEC Working Group meetings; reporting any significant findings to the BPA Manager for Security and Emergency Management; conducts periodic reviews of BPA external web pages, externally distributed documents, and participates in the NEPA review process.

G. **OPSEC Working Group** aids in the identification of CSI, determines vulnerabilities, assesses threats and risks, and recommends countermeasures; advises the BPA Manager for Security and Emergency Management and BPA Senior Management on the safeguarding of CSI and potential impacts to critical infrastructures; includes members from all Custodial Organizations. Each member is responsible for advising his/her respective managers and other key officials on OPSEC matters, as well as aid in the development of detailed guidance and procedures.

H. **Vice Presidents** are responsible and accountable for management of CSI/CII that is handled in their organizations; responsible for implementing and monitoring actions undertaken in support of this policy; designating a representative as a member of the OPSEC Working Group; supervising the development of additional OPSEC procedures specific to his/her organizational needs; establishing internal processes for clearing the release of CII for external use; clearly assigns key staff person(s) the responsibility for official review of CII and the identification of CSI prior to any external release;

responsible for all final decisions on the release of CSI, based on 'need-to-know' and accountability of risk, after consulting with the OPSEC Program Manager.

1081.5 PROCEDURES

Procedures and general guidance are addressed separately and can be found within 1081 Implementation Guidance. A copy can be obtained by contacting the Security Office, e-mail the OPSEC Program Manager or connect to the document via Security and Emergency Management's internal web link. Additionally, employees should contact their organization Vice President, or their designated representative, for additional guidance unique to their workgroup.

1081.6 REFERENCES

A. *Freedom of Information Act, 5 U.S.C. § 552 (2002).*

B. *Privacy Act, 5 U.S.C. § 552(a) (2002).*

C. *Title 42, United States Code, Section 5195c (USA PATRIOT Act).*

D. *Title 42, United States Code, Sections 4321 to 4370e (NEPA).*

E. *Executive Order 12958, as amended, Classified National Security Information, April 17, 1995.*

F. *Executive Order dated October 16, 2001, for Protection of Critical Infrastructure.*

G. *DOE O 471.2A, Information Security Program, March 27, 1997.*

H. *DOE O 471.3, Identifying and Protecting Official Use Only Information, dated April 9, 2003.*

I. *DOE O 5639.7, Operations Security Program, April 30, 1992.*

J. *DOE G 471.3-1, Guide to Identifying Official Use Only Information, dated April 9, 2003.*

K. *DOE M 475.1-1, Identifying Classified Information, dated May 8, 1998.*

L. *BPA OPSEC Plan, Revised April 30, 2002.*

M. *DOE Operations Security Guide 471.2-2, May 11, 2000.*

N. *National Security Decision Directive (NSDD) No. 298, National Operations Security Program, 1988.*

O. *North American Electric Reliability Council, Security Guidelines for the Electricity Sector: Protecting Potentially Sensitive Information, DRAFT, May 9, 2002.*

P. *Pacific Northwest Electric Power Planning and Conservation Act (Northwest Power Act), 16 U.S.C. § 839 (2000).*

Q. *FERC Regulations (for example 888, 889).*

R. *18 CFR, Part 375, The Commission, and Part 388, Information and Requests, dated April 1, 2003,*

S. *BPA Manual Chapter 1080, Operations Security*

T. *BPA Cyber Security Protection Plan, April 26, 2002.*

U. *DOE Memorandum from Deputy Secretary of Energy on Reviewing the Availability of Operational Information, October 26, 2001.*

V. *DOE Memorandum from Secretary of Energy on Safeguarding Information Pertaining to Weapons of Mass Destruction and Other Sensitive Information, May 30, 2002.*

W. *Memorandum from White House Chief of Staff on Action to Safeguard Information Regarding Weapons of Mass Destruction and Other Sensitive Documents Related to Homeland Security, March 19, 2002.*

X. *Memorandum from Information Security Oversight Office, NARA, and Office of Information and Privacy, U.S. Department of Justice, on Safeguarding Information Regarding Weapons of Mass Destruction and Other Sensitive Records Related to Homeland Security, March 19, 2002.*