Office of Compensation Analysis and Support Handling Controlled Unclassified Information	Document Number: OCAS-PLCY-0001 Effective Date: 1/22/2009 Revision No.: 00 Controlled Copy No.: _____ Page 1 of 17
Subject Expert: Tim Taulbee Approval: Signature on file Date: 1/22/2009 Stuart L. Hinnefeld, Health Science Administrator	Supersedes: None
Concurrence: Signature on file Date: 1/22/2009 Larry Elliott, Director OCAS, NIOSH	

TABLE OF CONTENTS

RECORD OF ISSUE/REVISIONS

ISSUE AUTHORIZATION DATE	EFFECTIVE DATE	REV. NO.	DESCRIPTION
1/22/2009	1/22/2009	00	New document to establish guidelines for the handling of sensitive documents and information. First approved issue.

1.0 PURPOSE

The purpose of this policy is to provide requirements for the receipt, access and use of controlled unclassified information [e.g., Unclassified Controlled Nuclear Information (UCNI), or Official Use Only Information (OUO)] received or generated in support of the National Institute for Occupational Safety and Health (NIOSH) responsibilities under the Energy Employees Occupational Illness Compensation Program Act.

2.0 SCOPE

This policy provides the framework for managing controlled unclassified information, information sources, and information technology to ensure that records created, received and maintained in support of the Project are handled in compliance with U.S. Department of Energy (DOE) directives and Federal regulations (e.g., 10 CFR part 1017).

This policy applies to all NIOSH employees, its contractors and subcontractors, and special Government employees, such as members of the Advisory Board on Radiation and Worker Health (ABRWH), who use this type of information and defines the steps necessary to ensure the protection and security of controlled unclassified information during use and disposition.

3.0 REFERENCES

3.1 DOE Order 471.1A, Identification and Protection of Unclassified Controlled Nuclear Information

3.2 DOE Manual 471.1-1, Identification and Protection of Unclassified Controlled Nuclear Information Manual

3.3 DOE O 471.3, Identifying and Protecting Official Use Only Information

3.4 DOE M 471.3-1, Manual for Identifying and Protecting Official Use Only Information

3.5 DOE G 471.3-1, Guide to Identifying Official Use Only Information

3.6 10 CFR Part 1017, Identification and Protection of Unclassified Controlled Nuclear Information

3.7 5 USC 552, Freedom of Information Act, as amended

3.8 42 USC 2168, Atomic Energy Act of 1954, as amended

3.9 Security Plan for Interviews Conducted in Support of the EEOICPA by NIOSH in concert with the Oak Ridge Associated Universities at DOE Oak Ridge Operations, December 2004, as amended.

4.0 RESPONSIBILITIES

4.1 Team Leader (Supervisor) - The Team Leader is responsible for authorizing access for personnel within his or her task who require access to the system on which controlled unclassified information is stored and ensuring that employees with such access adhere to the requirements established under this policy.

4.2 Project Records Custodian - A Project Records Custodian is identified, as necessary, by Project management and is responsible for oversight of the Records and Information Management Program for the Project. This is accomplished by interpreting regulatory requirements, establishing standards, generation of policies and procedures, and conducting periodic assessments for conformance to these requirements.

4.3 Employees - Employees are responsible for conforming with the requirements of this policy. Documented verification of an employee's awareness of this policy must be maintained and is subject to periodic internal and/or external assessment.

4.4 Classification Officer (CO), UCNI Reviewing Official (RO), and/or Derivative Classifier (DC) - A DOE-approved individual responsible for reviewing documents generated by this Project which may potentially contain classified or controlled unclassified information.

5.0 GENERAL

5.1 Controlled unclassified information is plain text or machine-encoded data that, as determined by competent authority (e.g., information owners), has relative sensitivity and requires protection because of statutory or regulatory restrictions (i.e., UCNI, OUO).

This is information that requires a degree of protection because inadvertent or deliberate misuse, alteration, disclosure, or destruction could adversely affect national security or other Governmental interests (e.g., program-critical information or controlled scientific and technical information, which might include computer codes [computer programs] used to process such information).

5.2 Thumb drives, flash drives, and other removable electronic media containing controlled unclassified information should be password protected and/or encrypted, especially when this information is removed from a Federal facility.

5.3 The two types of controlled unclassified information referenced in this policy are UCNI and OUO.

Unclassified Controlled Nuclear Information
This is not a classification category, and information subject to the UCNI handling restraints is not classified. However, information subject to UCNI handling is defined as certain unclassified but sensitive Government information concerning nuclear material, weapons, and weapons components. The dissemination of such information is controlled under section 148 of the Atomic Energy Act and must be protected from release to the general public.

Official Use Only
This is not a classification category and information marked OUO is not classified. However, this information may be exempt from public release under the Freedom of Information Act (FOIA) because the public release of such information 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 authorized activities. Such information is protected as OUO information under DOE directives.

5.4 Potentially Classified Information

Documents which are generated during the course of this project that have the potential to contain classified information in them are covered under the requirements of OCAS-PR-011, Department of Energy Classification Review of Documents.

In the event that any document encountered is suspected of containing classified information, the document must be protected and provided via hardcopy to the appropriate Department of Energy office. Instructions on how to proceed with that document will be provided by the DOE.

5.5 Violations

A violation is any knowing, willful, or negligent action that could reasonably be expected to result in the unauthorized disclosure of UCNI or any knowing willful, or negligent action to control information such as UCNI for prohibited reasons (10 CFR 1017.5). The person committing a violation is subject to a potential recommendation by DOE to impose a civil penalty or to seek imposition of a criminal penalty by referring the matter to the Attorney General for investigation and prosecution.

5.6 Security Clearance Training Refesher

All personnel who hold a DOE security clearance, including DOL and NIOSH employees and contractors performing EEOICPA-related work, must complete an Annual Security Refresher Briefing. Each clearance holder will receive an e-mail message from DOE notifying them of the requirement and providing instructions in how to access the briefing. The briefing is done electronically and is usually distributed in April or May of each year. The EEOICPA Project Manager will be advised of DOL and NIOSH employees who do not complete the briefing within the required period. Failure to complete the briefing could ultimately result in termination of the security clearance.

6.0 POLICY PROCESS

It is NIOSH policy that all employees (Federal staff, contractors and subcontractor staff and special Government employees) will follow the requirements established in the following paragraphs related to the use and disposition of UCNI and OUO material.

The originator of a document is responsible for transmitting a document to a CO, UCNI RO, or DC to determine the need for review.

Documents received from DOE facilities (e.g., through data capture efforts) should be marked according to their sensitivity level by the originating authority. See OCAS-PR-010 for more details.

6.1 Access to Unclassified Controlled Nuclear Information

Only employees authorized for routine or special access to UCNI may have access to such information.

6.1.1 Routine Access

Routine access refers to the normal exchange of UCNI during the conduct of official business and allows for further dissemination of UCNI if the requirements in paragraph 6.1.1.2 below are met.

6.1.1.1 Authorized Individual - An Authorized Individual, who might be the originator or possessor of UCNI, may grant routine access to another eligible person (see paragraph 6.1.1.2 for eligibility requirements) simply by giving that person the UCNI. No explicit designation or security clearance is required. The recipient of the UCNI becomes an Authorized Individual for that UCNI.

6.1.1.2 Eligibility for Routine Access - To be granted routine access to UCNI, a person must have a need to know the specific information as part of their performance of official duties or authorized activities. In addition to the need-to-know requirement, the person must meet at least one of the following requirements:

6.1.1.2.1 U.S. Citizen. The person is a U.S. citizen who is one of the following:

- A Federal employee.
- An employee of a Federal contractor or subcontractor.
- A special government employee who serves as an advisory committee member.
- A Member of Congress.
- A staff member of a congressional committee or of an individual Member of Congress.
- The Governor of a state, his/her designated representative, or a State government official.
- A local government official or an Indian tribal government official.
- A member of a State, local or Indian tribal law enforcement or emergency response organization.

6.1.1.2.2 Other than a U.S. Citizen. The person is other than a U.S. citizen and is one of the following:

- A Federal employee.
- An employee of a Federal contractor or subcontractor.
- A Federal consultant.

6.1.1.2.3 Other Than a U.S. Citizen and Otherwise Not Eligible for Routine Access. The person may be other than a U.S. citizen who is not otherwise eligible for routine access to UCNI material as described in paragraph 6.1.1.2, but who requires routine access to specific UCNI material in conjunction with one of the following:

- An international nuclear cooperative activity approved by the U.S. Government.
- U.S. diplomatic dealings with foreign government officials.
- An agreement for cooperation under Section 123 of the Atomic Energy Act.
- Provisions of treaties, mutual defense acts, or Federal contracts or subcontracts.

The authorized individual who desires to release UCNI material to a person for the reasons listed in this paragraph must coordinate such release with the DOE Secretarial Officer or NNSA Deputy Administrator or Chief with cognizance over the information.

6.1.1.3 Dissemination Limitations - An Authorized Individual may disseminate UCNI only to a person who is eligible for routine access to UCNI or to a person granted limited access to UCNI.

6.1.2 Limited Access

Limited access may be granted to individuals not authorized for routine access to UCNI. For example, limited access might be granted to an attorney representing an Energy Employee (EE) in litigation.

6.1.2.1 Submission of Request - A person not authorized for routine access to UCNI may submit a request for limited access to UCNI through the cognizant DOE security office. Per 10 C.F.R. § 1017.16(b) such requests must include the following:

- The requestor's name, current residence or business address, birthplace, birth date, and country of citizenship;
- A description of the specific UCNI requested;
- A description of the purpose for which the UCNI is needed; and

- Certification by the requestor of his/her understanding of, and willingness to abide by, the requirements in 10 C.F.R. pt. 1017 and understands that he or she is subject to the civil and criminal penalties specified in subpart F of 10 CFR part 1017.

A person granted limited access to specific UCNI as defined in this paragraph is not an Authorized Individual and must not disseminate the UCNI.

6.2 Determination and Handling of Unclassified Controlled Nuclear Information

An Authorized Individual who grants routine access to specific UCNI who is not an employee or contractor of the DOE must notify the person receiving the UCNI of the protection requirements specified in this section. The following requirements for protection and handling UCNI are from 10 CFR part 1017, DOE Order 471.1A, and DOE Manual 471.1-1:

6.2.1 Protection In Use

An Authorized Individual shall maintain physical control over any documents marked as containing UCNI to prevent unauthorized access to the information.

6.2.2 Protection in Storage

UCNI documents shall be stored to preclude unauthorized disclosure. Storage of such documents with other unclassified documents in unlocked receptacles, such as file cabinets, desks, or bookcases, is adequate if there is Government or Government-contractor internal building security during non-duty hours.

When such internal building security is not provided, locked rooms or buildings provide adequate after-hours protection. If rooms or buildings are not locked or otherwise controlled, UCNI documents shall be stored in locked receptacles, such as file cabinets, desks, or bookcases.

6.2.3 Reproduction

Authorized Individuals may reproduce UCNI documents without permission of the originator to the minimum extent necessary consistent with the need to perform their official duties. The reproduced documents must be marked and protected in the same manner as the original documents (see Section 6.3 for marking guidance). Employees shall use extreme discretion when sending electronic data containing UCNI to the printer(s), and must retrieve all printed information immediately from the printers to avoid inadvertent disclosure to unauthorized personnel.

In addition, Authorized Individuals shall clear copy machine malfunctions and check all paper paths for UCNI. They shall destroy excess paper containing UCNI as described below. In the event that a machine malfunction results in a call for service, an Authorized Individual shall accompany the repairman to ensure that all paper paths are properly cleared of UCNI.

6.2.4 Destruction

At a minimum, Authorized Individuals shall destroy UCNI material by using a cross-cut shredder that results in particles no larger than 1/4-inch wide and 2 inches long.

Note that the decision to dispose of any record information, whether it contains UCNI, must be consistent with the records management policies and procedures for records disposition within the agency.

NOTE: Employees must *not* dispose of UCNI documents in regular waste receptacles unless the documents are destroyed in accordance with the guidelines established in this policy.

6.2.5 Transmission

Authorized Individuals should transmit UCNI only by means that preclude unauthorized disclosure or dissemination.

6.2.5.1 Outside a Facility

To transfer UCNI documents outside a facility, Authorized Individuals shall:

- Package documents, regardless of media, marked as containing UCNI in a single, opaque envelope or wrapping.
- Use any of the following U.S. mail methods: U.S. First Class, Express, Certified, or Registered Mail.
- Any means approved for transmission of classified documents.
- Hand-carry the documents as long as he/she controls access to the UCNI.

6.2.5.2 Within a Facility

To transfer UCNI within a facility, Authorized Individuals shall:

- Use a single opaque envelope or wrapping. The address of the recipient and the sender must be indicated on the outside of the envelope or wrapping along with the words “To Be Opened By Addressee Only.”
- Hand-carry the document as long as he/she controls access to the UCNI.

6.2.5.3 Over Telecommunication Circuits

UCNI must be protected by encryption when transmitted by telecommunications services, including voice (telephonic, point-to-point), facsimile, narrative message, communications facilities, radio communications, and over public-switched broadcast communications paths (e.g., Internet).

This can be accomplished through DOE public key systems or use of encryption algorithms that comply with all applicable Federal laws, regulations, and standards that address the Key Cryptography and Key Management.

6.2.6 Automated Information Systems (AIS)

The AIS or AIS network must ensure that only Authorized Individuals are able to access UCNI. Networks interconnected with a public switched - broadcast network, such as the Internet, must provide provisions (authentication, file access controls, etc.) to ensure the protection of UCNI against unauthorized access. UCNI transmitted over broadcast networks like the Internet, where unauthorized access is possible, must have protection (e.g., encryption) to ensure that there is no improper access to the information.

6.2.7 Marking UCNI Documents

Document preparers shall apply UCNI markings to any unclassified material that contains or reveals UCNI regardless of any other control marking (e.g., Official Use Only, company proprietary) that is also on the document.

6.2.7.1 Front Marking

After determining that an unclassified document contains UCNI, the Reviewing Official marks or authorizes the front of the document to be marked as follows:

UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION

NOT FOR PUBLIC DISSEMINATION

Unauthorized dissemination subject to civil and criminal sanctions under Section 148 of the Atomic Energy Act of 1954, as amended (42 U.S.C. 2168)

Reviewing Official: _____
(Name/Organization)

Date: _____

Guidance Used: _____

6.2.7.2 Page Marking

Document preparers shall place the appropriate marking (UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION or UCNI) on the bottom of the front of the document, and on the bottom of each interior page of the document.

This marking may be in the Footer of an electronic document or otherwise marked on the top and bottom of each interior page of the document.

Only (1) the Reviewing Official who applied the markings or (2) the local Classification Officer or his/her delegates may authorize the removal of these markings.

Authorized users of UCNI who have been authorized by the Reviewing Official/Classification Officer to remove UCNI markings from a document that contains UCNI should maintain written documentation of such authorization and action.

6.2.7.3 Use of Other Markings

- Caveat

  An UCNI document may be marked with the caveat "DISSEMINATION CONTROLLED" when programmatic requirements place special dissemination or reproduction limitations on such information. This marking indicates that reproduction, extraction of information, or redistribution of such information requires the permission of the cognizant DOE program office. If this caveat is applied, the document preparer shall ensure that the following marking is placed immediately above the document's front marking:

  DISSEMINATION CONTROLLED

  When applied, it requires the permission of the cognizant DOE program office before reproduction, extraction, or redistribution of the document so marked takes place.

- Special-Format Documents

  Special formats of unclassified documents (e.g., photographs, viewgraphs, films, magnetic tapes, floppy diskettes, CDs, audio or videotapes, slides) shall be marked to the extent practicable as described in section 6.3. Regardless of the precise markings used in such cases, any special-format unclassified document that contains UCNI shall be marked such that both a person in physical possession of the document (e.g., markings on a viewgraph frame, a film reel and its container) and a person with access to the information in or on the document (e.g., markings on the projected image of a slide, a warning on a film leader) are made aware that it contains UCNI. When space is limited, the use of "UCNI" will suffice.

6.3 Determination of Official Use Only

The definition of OUO is taken from DOE Order 471.3, Identifying and Protecting Official Use Only Information, which defines OUO as a designation identifying certain unclassified but sensitive information that may be exempt from public release under the 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 authorized activities.

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 authorized activities; and fall under at least one of eight FOIA exemptions (2 through 9 listed in Attachment A); information falling under exemption 1 can never be OUO because it covers information classified by Executive order). (See DOE Guide 471.3-1 for additional details.)

Export Controlled Information (ECI) is a special category of OUO information. ECI is certain unclassified Government information under the Department of Energy's cognizance that, if generated by the private sector, would require a specific license or authorization for export under regulations. Information and technology regulated by the Export Administration Regulations, 15 CFR Parts 742, 744, and 746, and the International Traffic in Arms Regulations, 22 CFR 120.21.

6.3.1 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.

6.3.2 Protection in Storage

OUO documents shall be stored to preclude unauthorized disclosure. Storage of such documents with other unclassified matter in unlocked receptacles, such as file cabinets, desks, or bookcases, is adequate if there is Government or Government-contractor internal building security during non-duty hours.

When such internal building security is not provided, locked rooms or buildings provide adequate after-hours protection. If rooms or buildings are not locked or otherwise controlled, OUO documents shall be stored in locked receptacles, such as file cabinets, desks, or bookcases.

6.3.3 Reproduction

Authorized Individuals may reproduce OUO documents without the permission of the originator to the minimum extent necessary consistent with the need to perform their official duties. The reproduced document must be marked and protected in the same manner as the original document (see Section 6.3 for marking guidance). Employees shall use extreme discretion when sending electronic data containing OUO information to the printer(s), and must retrieve all printed information quickly from the printers to avoid inadvertent disclosure to unauthorized personnel.

In addition, Authorized Individuals shall clear copy machine malfunctions and check all paper paths for OUO. They shall destroy excess paper containing OUO as described below. In the event that a machine malfunction results in a call for service, an Authorized Individual shall accompany the repairman to ensure that all paper paths are properly cleared of OUO.

6.3.4 Destruction

At a minimum, Authorized Individuals shall destroy hard-copy OUO documents by using strip-cut shredders that result in particles of no more than 1/4-inch wide strips. Authorized Individuals shall use appropriate methods to destroy CDs that contain OUO information.

Note that the decision to dispose of any record information, whether it contains OUO, must be consistent with the records management policies and procedures for records disposition within the agency.

NOTE: Employees must *not* dispose of OUO documents in regular waste receptacles unless the documents are strip-shredded in accordance with the guidelines established in this policy.

6.3.5 Transmission of OUO

Authorized Individuals should transmit OUO only by means that preclude unauthorized disclosure or dissemination.

6.3.5.1 By Mail

When transmitting OUO by mail, use a sealed envelope and mark the envelope with the recipient's address, a return address, and the words TO BE OPENED BY ADDRESSEE ONLY. For mail leaving the facility, any of the following U.S. mail methods may be used: First Class, Express, Certified, or Registered Mail. Any commercial carrier may also be used.

6.3.5.2 By Hand

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 material.

6.3.5.3 Over Telecommunications Circuits

6.3.5.3.1 OUO should be protected by encryption when transmitted by telecommunications circuits whenever possible. This can be accomplished through DOE public key systems or use of encryption algorithms that comply with all applicable Federal laws, regulations, and standards that address the protection of sensitive unclassified information. 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

6.3.5.3.2 An unencrypted facsimile transmission must be preceded by a telephone call to the recipient so that he/she can control the document when it is received.

6.3.5.3.3 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 e-mail message. The sender must call the recipient with the password so that he/she can access the file.

6.3.6 Marking OUO Documents

A document determined to contain OUO information shall be marked as described in DOE Manual 471.3-1 and specified below.

6.3.6.1 Front Marking

After determining that unclassified matter contains OUO, the person making the determination marks or authorizes the front of the matter to be marked. Any employee from an office with cognizance over such information may determine whether such a document contains OUO information.

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: __

CDC FOIA Office review required before public release

Name/Org.: _____Date:_____

Guidance (if applicable)_____

6.3.6.2 Special format documents (e.g., photographs, viewgraphs, films, CDs, audiotapes, videotapes, CD-ROMs) must be marked so that persons possessing the documents and persons with access to the information in or on the documents are aware that they contain OUO information.

6.3.6.3 Documents determined to no longer warrant protection as OUO shall have their markings removed as described in DOE Manual 471.3-1.

6.3.7 Access to Official Use Only

6.3.7.1 Access to (1) documents marked as containing OUO information or (2) OUO

information from such documents shall be provided only to those persons who need to know the information to perform their jobs or other authorized activities.

6.4 Conduct of Interviews

6.4.1 The conduct of interviews of current or formerly cleared contractor and Federal employees of DOE for the purpose of gaining information and insight about DOE process operations in support of NIOSH-EEOICPA responsibilities is established in OCAS-PR-010, Requirements for Acquiring Department of Energy Information.

6.4.2 The provisions of this security plan for conduct of interviews which may involve discussion of classified and controlled information applies to all DOE Federal and contractor employees as well as NIOSH employees and its contractor employees/representatives and members of the Advisory Board on Radiation and Worker Health.

7.0 RECORDS

Information relating to the submittal of a document for review for classified or controlled information (e.g., date submitted, date returned) and the results of such reviews.

8.0 APPLICABLE DOCUMENTS

8.1 Drivers

Energy Employees Occupational Illness Compensation Program Act of 2000. Public Law 106-398; 42 USC 7384 et. seq. (as amended); 2000.

5 U.S.C. 552, The Freedom of Information Act

8.2 Forms

Verification of policy awareness (Actual form to be developed)

9.0 DEFINITIONS and ACRONYMS

DC – Derivative Classifier is a DOE approved individual responsible for reviewing documents generated by this Project, primarily Technical Basis Documents (TBDs), to determine whether they contain classified information.

BIOS – Basic Input/Output System

CD-ROM – Compact Disk-Read Only Memory

CFR – Code of Federal Regulations

CO – Classification Officer is a DOE approved individual responsible for administering the classification and UCNI programs at a DOE site.

DOE – Department of Energy [includes the National Nuclear Security Administration (NNSA)].

EE – Energy Employee, which is an individual who worked for an Atomic Weapons Employer or at a DOE facility.

FOIA – Freedom of Information Act, which is covered in Title 5 of the United States Code, section 552; enacted in 1966 to provide any person the right to request access to Federal agency records or information.

NIOSH – National Institute for Occupational Safety & Health

NNSA – National Nuclear Security Administration established to oversee and carry out the national nuclear security responsibilities of the Department of Energy.

OCAS – Office of Compensation Analysis and Support

OUO – Official Use Only, which is certain unclassified Government 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..

PC – Personal Computer

RO – Reviewing Official

TBD – Technical Basis Document, which is a report that focuses on a specific technical area describing the site with regard to some aspect of its worker radiation protection program, the environmental surveillance program, or the X-ray exposure equipment or techniques used to acquire X-rays for employment-required purposes. The parameters included in a TBD are ones that are needed to perform a thorough dose reconstruction related to the specific technical area of that TBD.

U.S. – United States

UCNI – Unclassified Controlled Nuclear Information, which is certain unclassified Government information concerning nuclear facilities, materials, weapons, and components whose dissemination is controlled under section 148 of the Atomic Energy Act.

ATTACHMENT A
OFFICIAL USE ONLY FOIA EXEMPTION CATEGORIES

For a more detailed discussion of the following exemption categories with examples, see DOE Guide 471.3-1.

Exemption 2 Internal agency rules and practices

Protects from disclosure of information that if disclosed would allow circumvention of a statute of agency regulation (e.g., policies for classifying documents).

Exemption 3 Prohibited by statute

Disclosure prohibitions contained in various Federal statutes (e.g., Atomic Energy Act).

Exemption 4 Trade secrets and other confidential business information

Protects from disclosure trade secrets and commercial or financial information obtained from a person, company, etc., that is privileged or confidential.

Exemption 5 Inter-agency or intra-agency communications protected by legal privileges; e.g., the deliberative process privilege, which includes advice, suggestions, evaluations, or recommendations concerning new or revised Government decisions and policies.

Exemption 6 Privacy information

Information involving matters of personal privacy (e.g., personal, medical, and similar files, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy).

Exemption 7 Certain types of information compiled for law enforcement purposes

Investigatory (e.g., ongoing reports).

Exemption 8 Information relating to the supervision of financial institutions

Records concerning examination, operating or condition reports prepared by, on behalf of, or for the use of an agency responsible for regulation or supervision of financial institutions.

Exemption 9 Geological information on wells

Records covering geological and geophysical information and data including maps concerning wells (e.g., new drilling techniques).