

**Jefferson Lab Supplemental Procedures for
DOE Official Use Only (OUO) Information**

GEN501

October 2008

Background and Purpose

Jefferson Lab has policies in place for the management of sensitive information and technologies as part of the Lab's Security Plan. The policy and procedures that specifically address the protection of sensitive information can be found in the Security Plan for Protection of Sensitive Information at <https://cc.jlab.org/policies/Security%20Plan%20for%20Protection%20of%20Sensitive%20Information.doc>.

On occasion Jefferson Lab provides DOE sensitive information that requires handling according to DOE Official Use Only (OUO) policies and procedures. In addition, occasionally Jefferson Lab staff are provided information from DOE that is marked "Official Use Only" or "OUO." The JSA contract for managing and operating the Thomas Jefferson National Accelerator Facility (TJNAF, Jefferson Lab) includes DOE Order 471.3 and DOE Manual 471.3-1 that detail the contractual requirements for managing OUO information. This document provides the Jefferson Lab procedures for both sending and receiving OUO information to and from DOE; in addition, this document serves as the training for staff working with OUO information.

Acknowledgment of understanding the content of this document is required and will be documented by following the URL at the end of the document.

Scope

This document addresses only the handling of DOE *OUO* information and does NOT address the handling of other specific types of information such as DoD *For Official Use Only* (FOUO), Export Control Information (ECI), International Traffic in Arms Regulations (ITAR), etc. Contact the CIO if you have any questions on any of these or other types of information that may have information control or security requirements.

Roles and Responsibilities

Chief Information Officer

- Provide systems designs, procedures, reviews, etc. for all systems and activities that involve the processing of OOU information

Designated Personnel

- Manage OOU information in accordance with Jefferson Lab procedures and contract requirements.
- Complete training as required to handle OOU information including acknowledgment of responsibilities.

All Staff

- Immediately inform supervisors and/or the CIO if OOU information is received by individuals who are not considered “Designated Personnel” for handling such information.

Definitions of Information Requiring OOU Designation for Transmitting to DOE or Other Labs

These definitions are provided early in this document in order to facilitate understanding of what is and is not OOU information. The Freedom of Information Act (FOIA) provides that “any person has a right, enforceable in court, to obtain access to federal agency records, except to the extent that such records (or portions of them) are protected from disclosure by one of nine exemptions ...” Documents that might be transmitted beyond the control of the JLab originator to DOE and/or DOE labs and that contain any information that meets the guidelines of these exemptions must be marked “Official Use Only” or “OOU.”

The full details on Exemptions 2-9 can be found in DOE G 471.3-1 at:

<http://www.directives.doe.gov/pdfs/doe/doetext/restrict/neword/471/g4713-1.pdf>

The following is a summary useful for most purposes. If you have any questions contact the CIO.

To be identified as OOU, information must be unclassified (Jefferson Lab does not have classified information) 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 DOE-authorized 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 FOIA exemptions (exemptions 2 through 9; information falling under exemption 1 can never be OOU because it covers information classified by Executive

order). These exemptions describe types of information whose unauthorized dissemination could damage governmental, commercial, or private interests.

Exemptions 2 through 9

2. Circumvention of Statute Exemption

Exemption 2 concerns information “related personnel rules and practices of an agency.” This exemption is for information that is predominantly internal to DOE and/or the Lab and where disclosure of the information could benefit someone who is attempting to violate a law or DOE regulation and avoid detection. Examples include Lab security and cyber security plans and operational activities.

3. Statutory Exemption

Exemption 3 covers information that is explicitly prohibited from disclosure by a statute passed by Congress. Basing an OOU determination on an exemption 3 statute is very complex and requires interpretations of statutory language and case law to ensure that the statute qualifies as an exemption 3 statute and that the document falls within the statute’s scope. Certain Export Controlled Information (ECI) may come under this exemption. Use of exemption 3 should be limited to those cases where appropriate statute-specific guidance is available and where you have conferred with the Lab’s Legal Counsel.

4. Commercial/Proprietary Exemption

Exemption 4 concerns “trade secrets and commercial or financial information obtained from a person and [that is] privileged or confidential.” Exemption 4 protects the interests of both the Government and persons submitting information to the Government. This exemption encourages commercial entities to voluntarily submit useful commercial or financial information to the Government and provides the Government with some assurance that the submitted information is reliable. Examples include procurement information in connection with bids, contracts or proposals that has been provided in confidence. This exemption includes trade secrets, inventions or other proprietary data that has been generated by the Lab or provided to the Lab by commercial vendors or potential vendors.

5. Privileged Information Exemption

Exemption 5 concerns “inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency.” Exemption 5 encompasses both statutory privileges and those commonly recognized by case law. The three primary privileges are deliberative process privilege, attorney work-product privilege, and attorney-client privilege, but the first issue to be addressed is whether the document can be considered an inter-agency or “intra-agency”

communication. Use of Exemption 5 should be reviewed by the Lab's Legal Counsel.

6. Personal Privacy Exemption

Exemption 6 concerns "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy." This exemption includes Personally Identifiable Information (PII) though the exemption is broader than PII. For the Lab's policy and definitions of PII see:

https://www1.jlab.org/mis/apps/pii_confirmation/pii_policy.cfm and
https://www1.jlab.org/mis/apps/pii_confirmation/pii_definition.cfm

7. Law Enforcement Exemption

Exemption 7 protects information compiled by an Agency with the authority to enforce civil statutes, criminal statutes, and statutes authorizing administrative proceedings. Any use of this exemption should be agreed to by the Lab's Security Officer and/or the Lab's Legal Counsel.

8. Financial Institutions Exemption

Exemption 8 protects frank evaluations of a financial institution's stability that might undermine the public's confidence in the institution or the relationship between financial institutions and supervisory agencies. Use of Exemption 8 should be reviewed by the Lab's Legal Counsel and/or Chief Financial Officer.

9. Wells Exemption

Exemption 9 concerns "geological and geophysical information and data, including maps, concerning wells." This exemption is rarely used but protects well information of a technical or scientific nature. Use of this exemption should be agreed to by the Lab's Security Officer and/or Legal Counsel.

General Procedures

1. All staff that handle OUO information shall have GEN501 "Handling OUO Information" in their Individual Training Plan (ITP) and the training shall be current, i.e. within the past year. The training shall include personal acknowledgment and acceptance of responsibility to meet the requirements for handling OUO information.
2. All offices, groups, departments and/or divisions that are approved to handle information meeting the FOIA exemptions shall have appropriate staff trained in the handling of OUO information.
3. All areas with OUO information shall have procedures to address the following items:
 - Physical security, e.g. physical access controls, appropriate storage spaces or containers, appropriate disposal facilities.

- Information security, e.g. controlling physical access to documents, locking documents in approved rooms and containers, and appropriately destroying documents by crosscut shredding or disposing in an approved disposal collection container.
 - Personnel security: processes that ensure that individuals have an authorized right or need-to-know for access to OOU information and appropriate training. Examples include contract labor to include end dates of the contract (Persons should not be given access beyond the end date of the subcontract, CRADA, or WFO).
4. At least annually the Lab’s CIO shall provide a documented self assessment of the Lab’s handling of OOU information and an audit of physical controls for all areas with OOU information.

Required Handling of OOU Information Including Destruction of OOU Information
 (See also: <http://www.directives.doe.gov/pdfs/doe/doetext/restrict/neword/471/m4713-1.pdf> for the full DOE Manual 471.3-1)

Hard Copy Information

- Mark documents that contain OOU information as follows:
 - Front Marking: The front marking includes the applicable FOIA exemption number and related category name (see list). The guidance referred to here is additional guidance that may be issued by DOE officials.

<p>OFFICIAL USE ONLY</p> <p>May be exempt from public release under the Freedom of Information Act (5 U.S.C.552, exemption number and category)</p> <hr style="border: 0.5px solid black;"/> <p>Department of Energy review required before public release</p> <p>Name/Org: _____ Date _____</p> <p>Guidance (if applicable) _____</p>

- Page Marking: Ensure that “Official Use Only” (or “OOU” if space is limited) is placed on the bottom of each page or, if more convenient, on just those pages containing the OOU information.
- Special Format Documents: Photographs, viewgraphs, films, magnetic tapes, CDs, DVD, etc. must be marked with “Official Use Only” (or “OOU” if space is limited).
- Transmittal Document: A document that (1) transmits an attachment or enclosure marked as containing OOU information and (2) does not itself contain OOU information must be marked on its front as follows to call attention to the presence of OOU information in the attachments or enclosures.

<p>Document transmitted Contains OOU information</p>
--

- Removal of OOU Markings: OOU markings applied based on guidance may be removed by any staff when the guidance used to make the determination states that the information is no longer OOU. (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 OOU. Once those deficiencies have been corrected, the OOU marking may be removed if appropriate.) 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 _____

- Hard Copies of OOU materials shall be in locked filing cabinets when not in use by approved personnel.
- OOU documents that are hand-carried out of the normal work area shall be concealed in an unmarked protective folder and properly controlled by a responsible person at all times.
- Documents marked as containing OOU information may be reproduced without the permission of the originator to the minimum extent necessary to carry out needed business activities. Copies must be marked and protected in the same manner as originals.
- OOU hardcopies must be destroyed by shredding in crosscut shredder or given to the Lab Security Officer for destruction.

Electronic Information

- All shared OOU documents must be kept in approved directories with access controls reviewed at least annually by the Computer Center.
- Backup CDs, memory sticks, etc. with OOU shall be treated the same as hard copies. IMPORTANT, no CD, memory stick, laptop, etc. may have PII without the documented permission of the CIO.
- Computers, laptops, etc. will be periodically surveyed by the Computer Center to be sure they are meeting requirements.
- CDs, memory sticks, computers, etc. with OOU information must be properly destroyed. Contact the Computer Center or give the physical items to the Lab Security Officer for destruction.

- OOU information transmitted over voice or data circuits should be protected by encryption 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.
- An automated information system (AIS) or AIS network must provide methods (e.g., authentication, file access controls, passwords) to prevent access to OOU information stored on the system by persons who do not require the information to perform their jobs or other Lab authorized activities.

Email

- The first line of an e-mail message containing OOU information must contain the abbreviation “OOU” before the beginning of the text. If the message itself is not OOU but an attachment contains OOU information, the message must indicate that the attachment is OOU. The attachment must have all required OOU markings.
- Email with OOU information requires that computer protections be set appropriately and that your email is managed as OOU. The Computer Center will periodically survey the security of your email and your system must be checked at least annually.
- Emailed OOU documents should be encrypted if possible. Contact the CIO if you need to email OOU information.

Release of OOU Information to DOE and other DOE Labs

- Release of JLab generated OOU informational outside the Lab requires that the office/group/department and/or division must have staff trained in handling OOU information including designated staff approved to release OOU information. In addition there must be appropriate logs or copies of the information.

I acknowledge and understand that DOE Official Use Only (OOU) information may be subject to restrictions by contract requirements between Jefferson Science Associates and the Department of Energy for operation of Jefferson Lab and by laws and regulations from multiple entities. I understand the policies, supplemental plan and procedures for management of this OOU information and that failure follow these procedures may result in personnel actions as delineated in the Jefferson Lab Administrative Manual.

Click button and fill in information to certify

