

**Jefferson Lab Free Electron Laser**  
**FEL Sensitive S&T Supplemental Security Plan and Procedures**  
**November 2007**

## **Background and Purpose**

Nearly all of the Lab's scientific and technical activities are exempted from any special security controls by the fundamental research exemption (National Security Decision Directive 189 of September 21, 1985, reinforced by then National Security Director Condoleezza Rice, who wrote to Association of American Universities co-chair Harold Brown in a letter dated November 1, 2001, that "[t]he policy on the transfer of scientific, technical, and engineering information set forth in NSDD-189 shall remain in effect, and we will ensure that this policy is followed."). However, special circumstances exist in the Free Electron Laser that may require the creation, sharing, and storage of information and technologies determined to be sensitive.

Science and Technology (S&T) is typically considered to be sensitive if the S&T involves activities or items on the Military Critical Technologies List (MCTL) or if the S&T is included in the Department of State's International Traffic in Arms Regulations (ITAR). Sensitive S&T has consequent export control requirements by law, regulation and the JLab DOE contract. Some Cooperative Research And Development Activities (CRADA)s and Work For Others (WFO) activities may have Department of Commerce export control requirements.

Jefferson Lab has policies in place for the management of sensitive information and technologies as part of the Lab's Security Plan. The policy that specifically addresses 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> .

Technical control plans with explicit controls, procedures and training are required for sensitive S&T to meet Department of State, Department of Commerce and/or Department of Defense regulations. The procedures in this plan provide requirements for those who have could handle sensitive S&T in the course of their duties at Jefferson Lab. This is to assure that similar information and technologies are protected according to statute, policy and our stakeholders' expectations. These policies and procedures are in addition to the standard security procedures that apply to all S&T at Jefferson Lab.

## **General Procedures**

1. Any areas with sensitive S&T requiring export controls shall have an area-specific supplemental security plan that addresses the following items:
  - Physical security, e.g. physical access controls, keeping documents locked up,

document shredding, etc.

- 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 involves persons who have an authorized right or need-to-know for access to controlled S&T 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). Similarly, non-U.S. citizens should not be given access beyond the end date established by their U.S. Citizenship & Immigration Service and Authority to work documents.
- The training shall include personal acknowledgement and acceptance of responsibility to meet the requirements.

2. For any area with sensitive S&T that requires participation of non-U.S. persons\* staff, users or other collaborators, a documented determination shall be made by the Export Control Officer, as to whether a Department of Commerce or Department of State export control license is required for the deemed export, i.e. an export to a non-U.S. person who is in the U.S. For these areas, only non-U.S. persons with appropriate licenses shall be allowed to participate in the activities and have access to the information and technologies.
3. At least annually for all areas with scientific and technical sensitive information and technologies, the Lab's Export Control Officer shall provide a documented self assessment of the associated security operations.

## Roles and Responsibilities

### Job Export Control Officer and Security Officer

- Consistent with responsibilities detailed in JLab's Export Control Procedures Manual, the Export Control Officer is responsible for reviewing all of the Lab's technology transfer documents such as CRADAs, Work for Others, and cooperative agreements. The Export Control staff serves as a resource to JLab employees in identifying Export Controlled equipment, technologies, and information.
- Maintain the FEL Science and Technology Supplemental Security plan, and act as a resource to FEL management and staff regarding sensitive and potentially sensitive S&T.
- Perform periodic reviews of S&T list and policies to assure compliance with security expectations of customers and stakeholders.
- Determines who in the Facilities and Logistics Management Group has access to the sensitive S&T areas and provides their training.
- Export Control Procedures can be found at <http://www.jlab.org/intralab/security/>

\* A US person is a citizen of the United States, a lawful permanent resident alien of the US (a "green card holder"), a refugee, protected political asylee or someone granted temporary residency under amnesty or Special

Agricultural Worker provisions. The general rule is that only US persons are eligible to receive controlled items, information or software without first obtaining an export license from the appropriate agency.

### FEL Division Leader

- Review FEL science and technology in consultation with funding programs, technical experts, and the Export Control Officer to determine what is sensitive. Along with principal investigators, lead scientists, and stake holders disclose in writing potential sensitive S & T information and technologies in all technology transfer planning documents.
- Determines who in the FEL Division has access to FEL sensitive science and technology.
  - Some personnel outside the FEL group who support FEL S&T and operations may also be designated as part of this list.
- Assure that all personnel have been properly trained and that policies and procedures regarding sensitive S&T are adhered to.

### Chief Information Officer

- Provide systems designs, procedures, reviews, etc. for IT systems containing sensitive S&T. Determines who in the IT Division has access to sensitive S&T.

### Designated Personnel

- Potential sensitive Scientific and Technical information and technologies shall be disclosed in writing in the technology transfer documents by the principal investigator or lead scientist.
- Manage sensitive S&T in accordance with Jefferson Lab security procedures.
- Complete training as required to handle FEL S&T sensitive S&T including acknowledgement of responsibilities.

## **Required Handling of Sensitive S&T including FOUO – ITAR Export Controlled Information**

### Hard Copy Information

- Mark any FEL sensitive information documents that you create as “For Official Use Only – ITAR Export Controlled” or FOUO – ITAR Export Controlled. Every page that is sensitive as well as the cover page must be marked (footer or watermark is okay).
  - Use “For Official Use Only” designation (DoD) rather than “Official Use Only” (DOE) as most of the FEL work is funded by DoD.
  - ITAR refers to International Traffic in Arms Regulations.

- Hard Copies of FOUO – ITAR Export Controlled materials shall be in locked filing cabinets when not in use by approved personnel.
- FOUO – ITAR Export Controlled 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.
- FOUO – ITAR Export Controlled hardcopies must be destroyed by shredding in crosscut shredder or given to the Lab Security Officer for destruction.
- Many documents from DoD only have the FOUO marking. Some of them have DoD Distribution C; this refers to limiting it to DoD and their contractors. All of these documents at Jefferson Lab shall be treated in the same fashion as FOUO – ITAR Export Controlled documents.
- If the activity involves a Department of Commerce export control license, then the documents should be marked “Business Sensitive – Export Controlled.”
  - Each CRADA or WFO with DoC export controlled or proprietary information shall include information security in its security plan.

### Electronic Information

- All shared FOUO – ITAR Export Controlled documents must be kept in a directory with access approved FEL Division Head and access provided by CIO.
  - The current directory is <\\jlabgrp\fel-adv> This will be updated in the future.
  - Encryption technology will be added to the system mid 2008.
- FOUO – ITAR Export Controlled documents on your desktop or laptop require that those systems be treated as FOUO – ITAR Export Controlled.
- Backup CDs, memory sticks, etc. with FOUO – ITAR Export Controlled shall be treated the same as hard copies.
- Computers, laptops, etc. will be periodically surveyed by the Computer Center to be sure it is meeting requirements.
- If the activity involves a Department of Commerce export control license, then the associated CRADA or WFO will include electronic information in its security plan.

### Email

- Email with FOUO – ITAR Export Controlled information requires that computer protections be set appropriately and that your email is managed as FOUO – ITAR Export Controlled. The Computer Center will periodically survey the security of your email. FOUO – ITAR Export Controlled documents that are emailed shall be encrypted using Microsoft security.

## Release to Other Parties

- Release of JLab generated FOUO – ITAR Export Controlled material or DoC export controlled material outside the Lab shall be approved via the two step process:
  - concurrence by the FEL Division Head, and
  - executing the standard review process by the cognizant program authority, typically ONR for ITAR export controlled materials, and CRADA or WFO specific requirements for those activities.

## **Experiments**

- Beginning in 2008, all FEL test plans will include a survey for sensitive S&T. Experiments involving sensitive S&T will require a security plan with sign -off by the FEL Division Head, and the Experiment's lead researcher.
  - A template will be provided at [\\jlabgrp\fel-adv\General\Sensitive\\_exp\\_template](\\jlabgrp\fel-adv\General\Sensitive_exp_template).
  - Control and operation of any sensitive S&T hardware shall be included in the plan.

## **Personnel**

- Export control licenses are being sought from either Department of Commerce or Department of State as appropriate to cover non-U.S. persons working on FEL sensitive S&T.
  - Non-U.S. persons may not work on export controlled sensitive S&T without a license.
- Conversations, exchange of information, etc. regarding FEL sensitive S&T can only be with appropriate DoD or DOE personnel including their contractors, or with Lab personnel on the approved list. See: [\\jlabgrp\fel-adv\General\Approved\\_personnel](\\jlabgrp\fel-adv\General\Approved_personnel)
  - A given CRADA or WFO activity will typically specify who has access to materials and information used for those specific projects.
- FEL Division Head can provide clarification for those who have questions about what is appropriate.

## **Physical Security**

- As of November 2007 FEL staff working on sensitive S&T are moving to a new trailer

located next to the FEL or to CEBAF Center. Access to the sensitive S&T trailer requires the following:

- Approval by the FEL Division Head, FEL Deputy Division Head, CIO or JLab Export Control and Security Officer.
- Completion of this course, GEN 503, or the IT version GEN 502, or the Facilities and Logistics version GEN 504.
- Temporary access for U.S. persons may be granted to areas with sensitive S&T trailer with the following procedure:
  - § Approval by the FEL Division Head, FEL Deputy Division Head, CIO or JLab Export Control and Security Officer.
  - § Escort by a trained staff member.
  - § Sign-in on the log book at the entrance to the trailer.
- The inside of the FEL trailer with sensitive S&T is an area where FOUO-ITAR Export Controlled documents can be freely moved about. However, in general it is a good practice to lock filing cabinets with sensitive S&T and office doors at night.

### Jefferson Lab Course GEN 503

I acknowledge and understand that sensitive science and technology (S&T) data may be subject to export controls restrictions by contract requirements with Jefferson Science Associates with the Department of Energy for operation of Jefferson Lab and by laws and regulations from the Department of Commerce and/or Department of State. I understand the policies, supplemental plan and procedures for management of this sensitive S&T and that failure follow these procedures may result in personnel actions as delineated in the Jefferson Lab Administrative Manual.

Click on the button and enter your information  
to record your certification



*(the pop-up blocker in your browser must be disabled)*