

GEN 503: Sensitive S&T Supplemental Security Plan and Procedures

January 2013

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 and some of the engineering activities 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 be sensitive as they may have Department of Commerce export control requirements. Mishandling of sensitive S&T can be a violation of federal laws and regulations and have associated legal ramifications.

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 link at <https://cc.jlab.org/security>

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 access or 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.

In addition to the procedures in this document, there may be physical location specific, network specific, etc. additional requirements. If so, these will be provided by your supervisor.

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 Science and Technology Supplemental Security plan, and act as a resource to areas of 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/> Also, contact Shipping and Receiving (5010) for assistance.

* 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 Ashlee 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.

Division Leaders

- Review 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.

- Determine who in the Division is permitted access to sensitive science and technology.
 - Some personnel outside the initiating Division who support sensitive 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 sensitive S&T including acknowledgement of responsibilities.

All Personnel

- All personnel are responsible to identify to their supervisor if you believe they are involved with handling sensitive S&T.

Required Handling of Sensitive S&T

Hard Copy Information

- Mark any sensitive information documents that you create as provided by your Division and supervisor for your specific program.
- Hard Copies of sensitive materials shall be locked in filing cabinets when not in use by approved personnel. There may be preapproved areas where sensitive materials including S&T can be out of cabinets during normal working hours.
 - Sensitive S&T 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.
 - Sensitive S&T documents in use shall be protected from casual viewing by unauthorized persons through physical control of the work area.
- Sensitive S&T 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 Statements; see: <http://www.dtic.mil/dtic/submit/guidance/distribstatement.html>
- 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 sensitive S&T electronic information and electronic systems shall be managed and accessed according to the specific plans and procedures provided by your Division and supervisor.
- Any removable media, such as backup CDs, memory sticks, etc. with sensitive S&T shall be treated the same as hard copies.
 - 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

- The Lab's email system can store / process sensitive information. However, the body of the messages and/or (as appropriate) the attachments should be encrypted as provided by your Division and supervisor for your specific program.
- As receipt of email with sensitive S&T cannot be controlled, users are responsible not to read sensitive S&T emails on devices that are not properly configured for sensitive information. Users should setup sensitive subfolders for sensitive S&T, immediately move any incoming sensitive S&T email to one of these folders, and never read sensitive S&T on devices not pre-approved for this use, such as mobile devices or any device not owned and managed by the JLab IT Division..
- Many email clients (Thunderbird, Mac Mail, etc.) automatically by default move copies of all email including attachments onto the local system. The Lab's Zimbra email system does not do this if the web browser interface is used. Before reading Lab email on an insecure system such as a home computer, contact the Computer Center for assistance in configuring it so as to not have copies of the email stored on an insecure computer.

Release to Other Parties

- Release of sensitive S&T outside the Lab shall be approved via the two step process:
 - Concurrence by the appropriate Division Head, and
 - Executing the standard review process by the cognizant program authority.

Personnel

- Export control licenses are sought from either Department of Commerce or Department of State as appropriate to cover non-U.S. persons working on 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 sensitive S&T can only be with appropriate DOD or DOE personnel including their contractors, or with JLab personnel on the approved list.
 - A given CRADA or WFO activity will typically specify who has access to materials and information used for those specific projects.
- Division Head can provide clarification for those who have questions about what is appropriate.

Physical Security

- Detailed physical security plans and procedures will be provided by the appropriate Division via the supervisors.

Jefferson Lab Course GEN 503

I acknowledge and understand that sensitive science and technology (S&T) data may be subject to export control restrictions under Jefferson Science Associates', management and operating contract with the U.S. Energy, as well as applicable laws and regulations from the U.S. Department of Commerce and/or Department of State. I understand the policies, supplemental plan and procedures for management of this sensitive S&T data. Failure to follow these procedures may result in disciplinary action up to and including termination from the Lab. Such violations may also result in criminal prosecution as specified by federal laws and regulations.

[Click and enter your
information to complete
this training and your
certification.](#)