NAME: _____ **COUNTRY:** _____

SPONSOR: _____ **DIV/GROUP:** _____ **PURPOSE:**_____

To be filled out by FACTS administrator
FACTS Visitor # _____ FACTS Request #_____

JEFFERSON LAB
Unclassified Foreign Visits & Assignments Program
GENERIC SECURITY PLAN
For Assignments

This plan complies with DOE Order 142.3A, the Department of Energy's Unclassified Foreign Visits and Assignments Program. Jefferson Lab is a DOE national laboratory for nuclear physics research. As a user facility for university scientists worldwide, its primary mission is to conduct research that builds a comprehensive understanding of the atom's nucleus. Derivative missions include basic and applied research using Free Electron Lasers. No classified work, information, or materials is permitted on site. No special nuclear materials are permitted on site and continuous export control/technology transfer screening is conducted to identify commodities, technology, and information that may be considered sensitive. Business, personal privacy and other information exempt from public release is protected by assigned custodians. The plan applies specifically to non-U.S. citizens on assignment whose country of origin is either a non-sensitive or sensitive country that has Jefferson Lab picture badged access or remote access to JLab's computing systems. The plan identifies DOE approved security measures for Jefferson Lab.

1. Purpose of Assignment (Circle all that Apply):

a. Research: (Experiment) (Research) (User)

b. Technology Transfer: (Cooperative Research and Development Agreement) (Research & Development Consortia) (Small Business Innovative Research) (Work for Others).

c. Support: (Commercial/Contractor Services) (Equipment Repair Installation) (Maintenance Services).

d. Employment: (Employment).

e. Other: _____

2. Subjects to be Discussed (List the subjects):

_____

_____

_____

3. Sponsor Certification: I understand I am to inform the foreign national of his/her responsibilities. This includes all requirements for entry approval and conduct, including the Security Plan; cyber security approval, export control and tech transfer reviews, and property protection. I understand I can obtain a copy of the DOE Office of Science UFV&A Hosting Guide and the JLab Generic Security Plan at the JLab Security Office.

Sponsors Name: _____

Sponsor's Signature & Date:_____

4. References:

a. Jefferson Lab Site Security Plan (SSP), approved by DOE, May 2013.
b. Jefferson Lab Cyber Security Program Plan (CSPP), DOE accreditation, January 2014.
c. DOE Order 142.3A, Unclassified Foreign Visits and Assignments Program, October 2010.
d. JSA/JLab Policy 301.05 Unclassified Foreign Visits and Assignments, Aug 2014.

5. Definitions:

a. Assignment. Non-U.S. citizen approved for unescorted access to Jefferson Lab for more than 30 consecutive days and is entered in FACTS.

b. Foreign National: An alien. For the purposes of DOE O 142.3A or its associated Contractor Requirements Document, an alien is a person who was born outside the jurisdiction of the United States, is a citizen of a foreign government, and has not been naturalized under U.S. law.

c. Host/Sponsor/Supervisor/Subcontracting Officer's Technical Representative (SOTR): These terms are interchangeable in the FV&A program. The JSA/JLab employee or DOE TJSO employee responsible for the day-to-day activities associated with the successful accomplishment of a visit or assignment. Except for nationals of state sponsors of terrorism, a foreign national who is a DOE employee or JSA/Jefferson Lab employee may be a host.

d. Sensitive Country National: A foreign national who was born in, is a citizen of, or employed by a government, employer, institution or organization, of a sensitive country. Countries may appear on the list for national security, nuclear nonproliferation, or terrorism support reasons. JLab will use the prevailing list posted at the DOE FACTS website. JLab Security & Services will provide the prevailing list to those needing access for official purposes.

e. Sensitive Subjects List (SSL): Unclassified subjects/topics identified in existing Federal regulations governing export control and by DOE as unique to its work; information, activities, and or technologies relevant to national security. Business, personal privacy and other information exempt from public release is protected by assigned custodians. JLab Export Control, Technology Transfer, and Cyber Security Subject Matter Experts stay abreast of changing Export Administration Regulations and continuously screen new JLab commodities, technologies, information, and technology transfer agreements for subjects that may adversely affect U.S. national and economic security.

f. State Sponsors of Terrorism (currently T-3 Countries; the number may change): Countries identified by the Department of State as sponsors of groups and/or activities which support terrorism or terrorist activities and are on the list of State Sponsors of Terrorism. JLab will use the prevailing list posted at the DOE FACTS website. JLab Security & Services will provide the prevailing list to those needing access for official purposes.

6. Applicable FV&A Security: This plan applies to all Sensitive Country Nationals and non-U.S. citizen assignees that are present at the laboratory for more than 30 consecutive days in a 12-month period or has remote access to JLab's computer systems. It does not apply to T-3 country nationals or non-U.S. citizens who

will be discussing sensitive subjects. Consult the JLab Facility Security Officer or Cyber Security Officer for a more specific security plan for T-3 national visits or those involving sensitive subjects.

7. Foreign Access Central Tracking System (FACTS): DOE's official national database of information on unclassified foreign visits and assignments. System access is controlled by the JLab Facility Security Officer.

8. Campus & Accelerator Site Security:

a. Campus Access: JLab campus has two 24-hour general access points to laboratory property ; Jefferson Ave and Lawrence Drive as well as Hogan Dr and Rattley Road. For your safety these entrances are monitored by recorded video cameras. Two other entrances off Hogan Drive are open from 6:30 AM to 6:30 PM during core workdays, Monday-Friday. During increased security conditions Lawrence Drive at Jefferson Avenue serves as the primary entrance to the laboratory.

b. Accelerator Site: All vehicles entering the Accelerator site are inspected on a random basis. Accelerator Site unoccupied buildings and Campus buildings are kept locked at all times, except during periods of active work process and individuals are visibly occupying the space. Normally occupied Accelerator Site buildings may be left unlocked from 7:00 AM to 6:00 PM on normal business days. These buildings include the Counting House (Bldg #97), MCC (Bldg #85), and FEL (Bldg 18). Occupants are responsible for unlocking and locking buildings. Security guards follow up to ensure doors remain locked and report discrepancies.

c. Badging Procedures: JLab picture badges serve as identification, authorize entry, and verify training. New JSA/JLab staff attend orientation on their start date and present valid photo identification and USCIS information. Users and contractors present REAL ID picture identification and USCIS information and complete Security and EH&S Orientation (SAF100) online during in-processing. Photo identification badges are issued and activated after completion of both Security and EH&S Orientation. JSA/ JLab employee supervisors/sponsors authorize access to controlled buildings, rooms, and labs. Certification of completion of the appropriate Annual Security Awareness training is required for continued JLab badged access to facilities. When the work is completed the JLab badge is disabled. JLab badge automated controls are not installed in all buildings and areas, keys may be issued by submitting a work order through sponsors/supervisors to Facility Management.

d. Briefing Non-U.S. Citizen Assignees: The JSA/JLab host will advise their guest(s) that he/she is their JLab official contact person and as such is responsible for the conduct and activities of the foreign national. The host must brief the foreign national on the following: compliance with all requirements for access approval and conduct, including timely, complete, an accurate information for FACTS, terms and conditions of access approval, including restrictions and requirements to notify the host of changes in name, immigrant/nonimmigrant status, of any civil or criminal problems that could affect their status and association with DOE, and that failure to provide appropriate documentation when required or providing fraudulent documentation will result in suspension of access approval, removal from site, and possible cancellation of future access. The JSA/JLab host will also brief on site escort requirements, identification and USCIS documentation verification requirements, DOE approval requirements for T-3 country nationals, proper use of JLab picture badges and controlled or prohibited items. These items include firearms; explosives, or other dangerous devices that pose a threat to people or property; controlled substances, Illegal drugs (and associated paraphernalia), and any other items prohibited by law.

e. Hosting Non-U.S. Citizen Visitors and Assignees (UFV&A): Only JSA/JLab employees can host non-U.S. citizens. T-3 country national assignees cannot host non-U.S. citizens. The DOE Office of Science UFV&A Host Guide is provided to all JSA/JLab employees and is posted on the JLab Security web page for reference. All non-U.S. citizen visitors should be referred to JLab Registration/International Services for identification and USCIS information verification.

f. Increased Security Conditions: The Homeland Security Advisory System provides a system of notifying Federal facilities to increase security precautions due to an increase in the national threat. Since Jefferson Lab is a U.S. Department of Energy facility, sponsors should advise visitors and assignees of increased security procedures as they are notified by JSA/ JLab's senior management.

9. DOE Computer/Cyber Access:

a. The Lab's cyber security program is fully incorporated in the Cyber Security Program Plan. The CSPP has been approved by DOE, the enclaves in the new CSPP have been Certified and Accredited, and the new CSPP is DOE approved. Both the existing and new CSPPs conform with the 205.x series of directives.

b. Names of Cyber Systems. The Assignee will have interactive access to the set of desktop, scientific computing, central systems, and support systems that are needed for the Assignee's research and are consistent with the Assignee's job responsibilities.

c. Time period of access. Cyber access is granted for the duration of the Assignee's active collaboration, contingent on on-going approval by the Assignee's Sponsor.

d. Risk Assessment. A general assessment of the Lab's risk and vulnerability posture is presented in the Lab's Site-Wide Risk Assessment. Given the controls referenced in Section E (see next section), the Assignee is in the general registered user risk group thereby providing minimal risk to the Lab's and DOE's cyber environments. Any additional risks associated with the Assignee, given the administrative and technical procedures described herein, are acceptable and are offset by the benefits provided by the Assignee's contributions to the Lab's and Collaborators' programs.

e. Identification of Access Controls. Access controls are based on N205.3-compliant passwords entered by means of the encrypted protocols documented in the CSPP. These currently include the use of SSL, SSH, and PKI certificates. In addition, see section 9.c above.

f. Cyber Approval. Access is granted to the Assignee to computing resources of Jefferson Lab as restricted by this document and as restricted by pertinent regulations of the DOE and the U.S. government.

10. Export Control: Export controls are designed to protect information important to international treaty participants. Export control rules govern the transfer of equipment, material, information, technical data and software to non-U.S. citizens regardless of where the transfer occurs. NOTE: Shipping JLab property to a foreign country, even if it originates from a foreign country, requires processing through JLab shipping and receiving. JLab employee foreign travel processing includes staff declaring JLab property (such as laptop computers) they intend to hand carry out of the country for business purposes. Screening is documented and a letter of authorization provided by the JLab Export Control Officer to pass through Customs.

11. Property: Each individual assignee is directly responsible for the property assigned them, including all activities affecting the property (transfer, loss, loan, damage, etc.). When a status change occurs (termination of employment or contract, lost property, relocation for longer than 5-working days, etc.) the responsible individual will follow procedures outlined in the property system. Assignees are responsible for alerting the JLab Property Manager of the in-house fabrication, acquisition, or shipment of high risk property. For further information contact the Property Manager at 269-5899.

12. UFV&A Subject Matter Experts: The following are contact persons for sponsors of Non-U.S. citizens.

a. Immigration: Visa & Immigration Administrator, 269-7687, or 269-6119
b. Security/Export Control: Security & Services Manager, 269-7548, or 269-7589
c. Counterintelligence: JLab Counterintelligence Officer, 269-5989
d. Technology Transfer: Tech Transfer Business Manager, 269-7027
e. Cyber Security: Cyber Security Manager, 269-6105