SITE-SPECIFIC COUNTERINTELLIGENCE

SUPPORT PLAN

FOR

THOMAS JEFFERSON NATIONAL ACCELERATOR FACILITY

AND

U.S. DEPARTMENT OF ENERGY

OFFICE OF SCIENCE

THOMAS JEFFERSON SITE OFICE

Dr. Cherry Murray. Director, Office of Science

Chuck Durant, Deputy Director, Counterintelligence Directorate
Office of Intelligence and Counterintelligence

October 2016

1) Executive Management

Objective. The U.S. Department of Energy (DOE) Counterintelligence (CI) Program is responsible to conduct CI activities designed to protect DOE federal and contractor personnel, resources, and information from intelligence collection on behalf of foreign powers or entities and against international terrorist activities. This site-specific CI support plan (SCSP) is tailored to address site-specific concerns and has been developed in coordination and cooperation between the Office of Science (SC), Thomas Jefferson Site Office (TJSO), Thomas Jefferson National Accelerator Facility (TJNAF) and the DOE Office of Intelligence and Counterintelligence, Counterintelligence Directorate, Forrestal Field Office (FFO).

Background. The TJNAF is funded by the Office of Science (SC) for the DOE with strong support from the City of Newport News, the Commonwealth of Virginia, and the United States Congress. As a user facility for scientists worldwide, its primary mission is to conduct basic research of the atom's nucleus at the quark level. The TJNAF is a non-nuclear, low hazard particle accelerator that conducts unclassified research that is published in open literature. TJNAF is managed and operated by Jefferson Science Associates LLC (JSA)) under contract DE-AC05-06OR23177 to the DOE. TJSO is responsible for day-to-day oversight of TJNAF operations and activities. The DOE security interest at TJNAF is limited to protection of federal and contractor personnel and government property used in support of unclassified nuclear physics research and development.

Intent. In order for the successful implementation of this site-specific CI program at TJNAF, a mutual understanding and effective relationship between on-site DOE and TJNAF management and the FFO Senior Counterintelligence Officer (SCIO) must exist concerning the nature and purpose of the CI program and its activities. In accordance with this SCSP, the DOE FFO is responsible to provide appropriate CI assistance and support in accordance with the level of risk at TJNAF. In carrying out this activity the intent is to support effective and successful scientific research, which is the primary mission of TJNAF. The SCIO, TJSO Manager, and TJNAF Director will collaborate to ensure this intent is met while appropriate CI activities are successfully accomplished within the tailored approach of this SCSP.

Authority. This SCSP incorporates guidelines and requirements of Executive Order 12333, "U.S. Intelligence Activities", the Secretary of Energy's Counterintelligence Plan, DOE Office of Counterintelligence Strategic Plan, and DOE O 475.1, Counterintelligence Program, dated 12/10/04.

Requirements. The TJNAF CI Program is managed jointly by SC, TJSO, TJNAF and the SCIO for the servicing CI office, which is the DOE FFO; as set forth in the DOE Order O 475.1, its Contactor Requirements Document and this SCSP. FFO will conduct their primary activities with the support and coordination of SC, TJSO and TJNAF management and personnel. The TJSO Manager and TJNAF Director will ensure necessary support is provided to the FFO to ensure effective implementation of this SCSP.

FFO will:

Conduct CI activities summarized in section 3 below, to protect TJSO and TJNAF information (e.g. unclassified controlled information, proprietary, unclassified, and economic information affecting national security), personnel, technologies and assets from international terrorist activities and from intelligence collection by or on behalf of foreign powers or entities.

The CI areas and activities that FFO will provide assistance and support to TJSO and TJNAF includes:

a. Information Technology (IT);
b. CI/CT Awareness Assistance;
c. Briefing and Debriefing Assistance;
d. Investigations and Inquiries;
e. Liaison;
f. Unclassified Foreign Visits and Assignments (UVFA) Program Support; and
g. Security Support.

Note: This plan reflects the graded approach called for in DOE O 475.1, based on the perceived level of risk or threat and type of activities at TJNAF. The graded approach is primarily reflected in the nature of the resource commitment to the CI activity and the level of resulting site/lab supporting activity. Specifically, there are no on-site CI personnel and the FFO commitment to TJNAF activities is part-time. As a result, activities on-site will be limited and focused on select individuals and activities, which most likely will assist in identifying activities of concern to CI. For matters where specific information of concern emerges, FFO will act quickly to carry out its CI support responsibilities.

TJSO/TJNAF Management will:

a. Ensure necessary on site support for CI activities and access to site personnel and facilities is provided to FFO personnel, as appropriate;
b. Interface as necessary with CI personnel to provide coordination, information or access to site resources that have an appropriate nexus to CI activities, (such as key personnel or computing resources) in accordance with the aforestated authorities;
c. Designate a TJNAF CI Representative for TJSO and/or TJNAF who will serve as the day-to-day interface for FFO to coordinate with on CI Program implementation activities; and
d. Ensure that SC, TJSO and TJNAF responsibilities with respect to this SCSP are effectively implemented.

2) Administrative Requirements

This section identifies administrative related activities and other requirements associated with the administration and implementation of the TJNAF SCSP.

2.1. TJNAF does not conduct classified work and most employees do not possess clearances (access authorization). There are a few TJNAF employees that do possess clearances and who will be provided threat awareness briefings and related information and in support of CI/CT matters. Additionally, TJSO and/or TJNAF will inform FFO of individuals who obtain clearances through DOE or other agencies either for on-site of off-site work to ensure these individuals also receive appropriate CI Awareness information.

2.2. Primary CI Advisor. The primary advisor for the TJSO and TJNAF is the SCIO for FFO. FFO staff assigned to support the CI program at TJSO/TJNAF is an extension of site staff. FFO staff will comply with all applicable TJNAF site requirements. The FFO SCIO, SC, TJSO, and TJNAF management will coordinate on the administrative requirements to support work on-site by the CI support staff from FFO. All management issues associated with the implementation of this SCSP should be addressed with the SCIO. The SCIO will interface with the TJSO Manager, TJNAF Director and/or the TJNAF CI Representatives as necessary to support an effective CI program at TJNAF. In those instances that may require solicitation and concurrence at the OCI HQ's level the SCIO will conduct and coordinate said matters with the Director, OCI and the TJSO Manager. As delineated in DOE O 475.1, the TJSO Manager is to also maintain effective coordination with the OCI Director on matters of CI interest.

2.3 TJSO Manager and TJNAF Director will ensure full support of the TJNAF CI program by site staff in accordance with aforementioned authorities, this SCSP, and DOE O 475.1.

2.4. Records Management. As appropriate, TJNAF will maintain any unclassified records necessary to support and document the implementation of the SCSP and related activities associated with the FFO. All classified related information and other matters associated with TJNAF will be secured at the FFO or at a support location in the nearby geographic areas. Selected classified matters will be made available to the TJSO and TJNAF officials to ensure an appropriate awareness of matters with a bearing on TJNAF activities or broader matters which may impact the site at some point.

2.5 Unique Access Program (UAP). Since TJNAF does not conduct classified or sensitive work and has a very few clearances, the standard DOE unique access program criteria are not applicable. For the purposes of the TJNAF CI program, a list of clearance holders and key management staff will be reviewed annually. Special CI support will be given to frequent sensitive country travelers and hosts.

3) Site-Specific CI Support Plan Implémentation - FFO

FFO will conduct the following CI related activities in aforementioned authorities and requirements for the TJSO and TJNAF.

3.1 Implement the CI Program and related policies, standards, and guidelines pursuant, provisions of this SCSP, DOE CI directives and other applicable requirements.

3.2 The FFO will serve as primary CI advisors and provide CI support and assistance to the TJSO and TJNAF management in accordance with established local/servicing CI office areas of responsibility. Regularly inform TJSO and TJNAF management of CI activities on-site. Ensure that site support is also in accordance with overall CI Program requirements.

3.3 Threat Analysis. TJNAF conducts only unclassified fundamental scientific research and development intended for public domain distribution; that is, TJNAF performs basic and applied research in science and engineering that is not subject to access, dissemination, or participation restrictions. The SCIO to TJNAF supports analyses of the threats posed by foreign intelligence services and international terrorist activities for CI purposes and provides threat information to TJNAF and DOE management to support the protection of personnel, information, facilities, and assets at TJNAF. The SCIO also provides relevant threat information to CI investigative, training and awareness, and Information and Special Technology Program (ISTP) personnel and outside offices such as those involved in foreign visits and assignments and other national security–related duties.

FFO will perform CI/CT threat assessments of the potential threat(s) associated with TJNAF from foreign intelligence collection and international terrorist activities. This threat analysis or assessment will be tailored to TJNAF and will support prioritization of local and national CI Program activities. This assessment will be updated every three years. Appropriate TJSO and TJNAF officials possessing authorized access will be provided the results of this threat analysis. Additional informal updates will be provided as warranted, normally in conjunction with routine site visits, based on changes in the threat environment. Threat analysis will be provided to outside offices such as those involved in the execution of the foreign visits and assignments, security, and hosts / and other potential national security related activities.

NOTE: The primary activity involved in conducting a site-specific threat analysis will be interviews with select site personnel and collection of basic information about site activities that are germane to assessing the vulnerabilities at TJNAF.

3.4 Information Technology (IT). TJNAF's cyber security program is described in the TJNAF Cyber Security Program Plan, which has been approved by TJSO. This plan details TJNAF's plans for countering the threats to information systems posed by all adversaries be they foreign intelligence collection and international terrorist activities or those posed by groups of domestic origin. The SCIO will remain in contact with TJNAF's Cyber Security program. The SCIO will advise TJNAF's Cyber Security program of specific threats or new trends in foreign intelligence or foreign terrorist cyber activities.

TJNAF conducts fundamental research that is unclassified and published in the open literature; as a result, the primary focus of cyber security at TJNAF is integrity of the data and protection from disruption of service. While TJNAF has indirect connectivity to DOE laboratories with higher sensitivity levels, there is no trust relationship involving access to classified or sensitive information.

As with all DOE records and facilities maintained by TJNAF, the TJNAF Chief Information Officer and TJNAF Cyber Security Manager have the appropriate (legally authorized and contractually appropriate) access to IT related records and facilities required for the performance of their official duties.

The FFO Cyber Technical Expert, under the direction of the SCIO, will liaison with key TJNAF cyber security personnel to provide awareness of relevant CI Cyber and cyber security issues, to respond to anomalous activity that may have a CI nexus, and for the purpose of coordinating activity related to the Inquiry Management and Analytical Capability (IMAC) deployed at TJNAF. The IMAC analyzes incoming and outgoing data packets for size as well as patterns.

3.4.1 The primary purpose of this is to counter the threat to information systems posed by foreign intelligence collection and international terrorist activities.

3.4.2 FFO will assist in the proactive integration and use of information security and intrusion detection capabilities to protect TJSO and TJNAF information architecture and to detect and deter technical attacks and intelligence gathering activities directed against said entities by hostile foreign intelligence and international terrorist elements.

3.4.2.1. FFO will provide analysis and recommendations regarding foreign collection patterns detected through the IMAC coverage of the TJSO and TJNAF. To facilitate this analysis the "Local Site Data" option of the TJSO / TJNAF IMAC system will be configured to store a local copy of all data on the FFO IMAC analysis server located at the DOE-HQ data center in Germantown, MD.

3.4.2.2. To further enhance site CI and Security capability for computer networks and to support traffic analysis capability FFO will provide the CI for Statistical Analysis of Mail Headers (CI-SAMH) sensor capability to the site. Similar to the IMAC capability, installed and operating outside the TJNAF network, FFO will work with site cyber security personnel to conduct analysis and share data to analyze and assess the derived information. The SAMH system analyzes for patterns in data elements within message headers such as "From:" "To:" "cc:" etc.

3.4.3 FFO will provide counterintelligence guidance to respond to unusual unsolicited email that possesses a foreign nexus. Also, FFO will provide pertinent counterintelligence guidance regarding the utilization of laptops, blackberries, palm pilots and other PDA devices while on foreign travel. FFO will assist in the development of a baseline for computer hardware exposed to a foreign environment, and coordinate in the analysis of any hardware suspected of overseas tampering.

3.5 CI / CT Awareness.

3.5.1 FFO in coordination with appropriate TJNAF staff will develop a tailored CI/CT awareness effort for the site. Awareness Program, which will be directly tailored to TJNAF and to include:

3.5.2 Executive Management Awareness. The SCIO and the CIO assigned to support TJNAF will assist the Lab in the development and/or implementation of an Executive Management Awareness briefing. The purpose of this awareness briefing is to ensure that TJSO and TJNAF management receive briefings on sensitive matters relating to site CI activities with at least an annual specific site CI update. As part of this effort, the SCIO briefing will ensure site management /executives are aware of their responsibilities associated in support of the CI Program.

3.5.3 Annual Basic Awareness Training. The SCIO and the CIO assigned to support TJNAF will assist in the development and/or implementation of an Annual Basic Awareness training briefing. All laboratory employees will be provided annual awareness training covering CI reporting requirements and other appropriate CI related information. This information will be developed in full coordination with TJNAF.

3.5.4 Comprehensive Awareness Training. In those instances where employees obtain a DOE or other agency security clearance, employees will receive comprehensive CI awareness briefing by the SCIO or CIO assigned to support TJNAF, tailored for their activities.

3.5.5 Annual Specialized Awareness Training. FFO will assist TJSO and TJNAF management to identify select groups of individuals for tailored CI / CT awareness. These groups could include key executives, frequent travelers, sensitive country foreign national hosts, security personnel, system administrators, and individuals involved with Cooperative Research and Development Agreements (CRADAs) or similar focused groups. These briefings would be succinct and tailored to the group. Specialized topics such as CI/CT threats to DOE science laboratories and personnel and economic espionage will be included as needed.

3.5.6 CI Quarterly Newsletter. The newsletter will be distributed via email to appropriate employees. Hard copies will be placed in select common areas.

3.5.7 CI Awareness Bulletin. Provide a periodic awareness bulletin to selected employees.

3.6 Briefing and Debriefing. The SCIO and/or the CIO assigned to support TJNAF will assist TJNAF in the briefing and debriefing of personnel whose activities require foreign

travel, hosting foreign visitors or assignees, interacting with sensitive country foreign nationals while on travel, or working in positions dealing with sensitive or proprietary technology or export control, or who otherwise need focused CI program support.

3.7 Investigations and Inquiries. Conduct investigations and inquiries in accordance with the aforementioned authorities as necessary to determine foreign intelligence or terrorist activities targeting of TJSO and TJNAF personnel, information or resources. In order to facilitate investigative activity, TJSO and TJNAF will provide access to DOE records and related information as required. FFO will coordinate investigative matters and related requests with appropriate TJSO and TJNAF management and/or CI Representatives. FFO will also coordinate its investigative activities with those of the FBI as required.

3.8 Liaison. Conduct liaison with site counterparts as appropriate (e.g., TJNAF CI Representative, executive management, security, cyber, export control, technology transfer). FFO will work aggressively to maintain and effective relationship with key site personnel concerning the CI program in support of TJSO and TJNAF. In addition, FFO will enhance existing liaison with the FBI, other members of the intelligence community, and local law enforcement as necessary to protect TJNAF personnel, programs and facilities.

3.8.1 FFO will interact with local, state and United States intelligence community (USIC) and law enforcement agencies concerning CI matters and in support of the site CI Program.

3.8.2 The TJNAF Facility Security Officer/TJNAF CI Representative is the primary local contact for Commonwealth of Virginia district court system and the City of Newport News public safety officials; sheriff's department, law enforcement, fire/rescue, and emergency management. For professional continuity, the FFO and TJSO CI Representative will coordinate on matters where there is a TJNAF related mission need to interface with these agencies.

3.8.3 FFO, TJSO and TJNAF CI Representatives will share relevant information as appropriate. TJSO and TJNAF will advise FFO through its normal interactions of significant site issues that may have a CI nexus or where CI can provide an advisory role to include but not limited too; information on operational and business activities, site security matters, foreign interactions, significant personnel matters, information concerning CRADA or other propriety information on site, Strategic Partnership Projects, significant new business that might change the site security posture, and other matters that site executive management believe is pertinent.

3.8.4 FFO will interface with TJSO and/or TJNAF site management or appropriate POC, and with the TJNAF Technology Review Committee (JLTRC) through the Technology Transfer Manager, as appropriate, to stay current with the issues reviewed by the committee and provide CI expertise and advice to the process to evaluate areas of potentially sensitive technology.

3.9 Unclassified Foreign Visits and Assignments (UFVA) Program Support. Coordinate and assist in UFVA matters in support of the site CI Program.

3.9.1 In support of an effective implementation of the local UFVA program, FFO will review and assess the CI risks associated with sensitive country foreign visits and assignments. FFO will provide CI advice, as appropriate, to the site approving officials, as necessary.

3.9.2 Review assignments in Foreign Access Central Tracking System (FACTS), as appropriate, and provide support to the approval process of specific visits and ensure intelligence community indices checks are conducted when required.

3.9.3 As necessary, provide CI consultations to the approval authority to evaluate foreign national access in the absence of the required completed indices check, and document that the consultation was conducted in the FACTS.

3.9.4 Assist TJNAF in conducting briefings and debriefings of hosts/sponsors/escorts of foreign visitors and assignees and in the development and implementation CI awareness modules/briefings for local UFVA training.

3.9.5 Assist TJNAF in support of the approval process for nationals of state sponsors of terrorism visits within OCI in coordination with procedures established by the Secretary.

3.9.6 As appropriate, assist TJSO, TJNAF and TJNAF Registration/International Services (JRIS) Office in support of an effective UFVA program by providing appropriate CI support.

3.9.7 TJSO and TJNAF will provide access to FFO for site visit and assignment information to support its activities.

3.10 Security Support. As appropriate, assist TJSO Security Manager and TJNAF Security Manager on matters related to the support of the TJNAF Physical and Personnel Security and CI Programs.

3.10.1 Maintain a close working relationship with the TJSO Security Manager.

3.10.2 Provide CI and CT information that directly impacts on TJNAF Site resources.

3.10.3 As appropriate, TJSO and TJNAF Security will provide FFO notification of security incidents so that FFO can act as a CI advisor to mitigate related risks.

3.10.4 As appropriate, FFO will interface with TJNAF security staff to assist as a CI advisor in support of security policy development.

3.11 Foreign Travel. Coordinate and assist in foreign travel matters in support of the site CI Program.

3.11.1 FFO will use DOE approved systems, [i.e., the Foreign Travel Management System (FTMS)] to review TJSO and TJNAF foreign travel activity and to determine the necessity of a personal travel pre-briefings or debriefings based upon travel destination, potential CI/CT threat issues and the sensitivity of the employee's assigned work, as appropriate.

3.12 Training. In coordination with the TJNAF CI Representative, the SCIO will provide the TJNAF CI Representative and other selective TJNAF staff applicable training and development necessary to execute their particular duties in support of the overall CI objectives. Local site-specific CI related training needs would be determined between TJSO, TJNAF management, with support from the FFO. TJNAF will provide appropriate training so that FFO staff supporting the site meets site general employee training requirements to afford regular access to the site.