Appendix 7

Jefferson Lab

Unclassified Foreign National Access Program Plan

5 June 2023

U.S. DEPARTMENT OF ENERGY

JSA

Prepared for the U.S. Department of Energy under Contract DE-AC05-06OR23177

Unclassified Foreign National Access Program

September 30, 2021

Submitted by:

Brian Hanlon, Security and Services Manager — 20 Sept. 2021 (Date)
Jefferson Science Associates
TJNAF Facilities Management and Logistics Division

Reviewed by:

Rusty Sprouse, Facilities Management and Logistics Manager — 28 Sept 2021 (Date)
Jefferson Science Associates
TJNAF Facilities Management and Logistics Division

Approved by:

Michael W. Maier, Chief Operating Officer — 30 SEPT 2021 (Date)
Jefferson Science Associates
TJNAF

Revision History		
Rev.	Date	Reason
1	5 June 2023	Corrected Security Plan Appendix Numbering

Table of Contents

1.0 Introduction 4
2.0 Exemptions 4
3.0 UFNA Requirements Implementation at TJNAF 6
3.1. Documentation 6
3.2. Lawful Immigration Status 8
3.3. Nationals from a Country(ies) of Risk 9
3.4. Nationals from a State Sponsor of Terrorism (SST) 10
3.5. Indices Checks 11
3.6. Access Requirements and Approvals 12
4.0 UFNA Responsibilities at TJNAF 13
4.1. Thomas Jefferson Site Office 13
4.2. Jefferson Science Associates 13
5.0 Definitions 15

Table of Figures

Table 1 – Guest Certifications 7
Table 2 – Host Certifications 7
Table 3 – TJNAF UFNA Requirements 12
Table 4 – TJNAF Subject Matter Experts 14

Unclassified Foreign National Access Program

References:

- DOE O 142.3B, CRD, Unclassified Foreign National Access Program
- TJNAF Administrative Manual, Guest Access Policy
- Ibid., Staff Access Policy
- Ibid., Meeting and Conference Policy

1.0 Introduction

The objective of the Unclassified Foreign National Access Program (UFNA) is to enhance Thomas Jefferson National Accelerator Facility's (TJNAF, aka Jefferson Lab) security by establishing an effective identification, verification, tracking, review, and approval process for non-U.S. citizens (hereafter, "foreign nationals") to access facilities, information, and technologies in support of Department of Energy (DOE) missions and goals. The program enables effective and efficient partnerships between DOE, TJNAF, industry and university collaborators, employees, students, scholars, and scientists to participate fully in lab operations, and to leverage TJNAF's science and technology as well as the U.S. higher education enterprise.

This appendix, therefore, addresses the UFNA program in the context of the Site Security Plan, which applies a risk-based protection strategy. DOE-approved security measures for the lab relating to foreign national access are outlined in this sub-program plan, which will be reviewed periodically and as required by changes in the order.

Except for the circumstances described in section 2.0 below, all guests must register in accordance with the Guest Access Policy, Administrative Manual 301.05, which provides the instructions for how both U.S. citizen and foreign national guests request and receive their access privileges. A companion policy provides instructions for how Staff members request and receive their access privileges.

JSA is required to promulgate to subcontractors, at any tier, the requirements of the Contractor Requirements Document (CRD)—and that to the extent necessary to ensure JSA's compliance with the requirements.

2.0 Exemptions

The following circumstances exempt TJNAF from compliance with the UFNA program requirements in accordance with the CRD, Attachment 1, Paragraph 2:

- Unclassified events and activities outside the U.S. or its territories (DOE Order 142.3B CRD (2)(a)).
- Dual citizens, only if one citizenship is the U.S. (DOE Order 142.3B CRD (2)(b)).
- Requests for access to information that is already in the public domain in accordance with applicable procedures. [NOTE: Physical access to TJNAF will follow the procedures in the Guest Access Policy and this Program Plan.] (DOE Order 142.3B CRD (2)(c)).
- Requests for access to information (e.g., technical specifications, project data, and

research results) for foreign nationals from countries that are formally part of a specific DOE program-sponsored international agreement. This applies only to information generated under these projects and agreed to be shared among the participants (DOE Order 142.3B CRD (2)(d)).

- Anyone attending a public event at TJNAF or off-site, or virtually (DOE Order 142.3B CRD (2)(c) and (e)).
- Certain activities within a General Access Area (GAA):
  - Personal visits (DOE Order 142.3B CRD (2)(f)(1)).
  - Third-party events (i.e., not related to TJNAF's mission) hosted on-site (DOE Order 142.3B CRD (2)(f)(2)).
  - Foreign national subcontractors performing construction activities (DOE Order 142.3B CRD (2)(f)(4)).
- Emergency responders and medical personnel called to TJNAF for an actual or simulated emergency (DOE Order 142.3B CRD (2)(g)).
- Anyone 17 years of age or younger and not involved in work-related activities at TJNAF (DOE Order 142.3B CRD (2)(h)).
- Personal visits, VIPS, delivery, service, and vendor personnel when escorted by a JSA employee qualified to prevent access to sensitive information, technologies, or equipment (DOE Order 142.3B CRD (2)(f)(3)) outside a GAA.

All virtual (online) audio and video conferences hosted by TJNAF staff to discuss information not protected by statute, regulation, or DOE policy—and determined releasable to the general public—*are considered public events under the CRD(2)(c) exemption*. When using virtual conferencing platforms, staff shall *not* discuss information that is not otherwise releasable to the public. Additional exempt circumstances include the following:

- Impromptu virtual meetings or technical discussions with TJNAF staff.
- Sharing unrestricted technical data through the normal scientific discovery and experimental process.
- Access to TJNAF information systems not requiring a user login and password.

Public events, as noted above and defined in Section 5 of this plan, include only information that is not protected by statute, regulation, or DOE policy and is determined to be releasable to the general public, and held in locations that are accessible to the general public (DOE Order 142.3B CRD(Att. 2)(22)).

Meeting and conference organizers must follow guidance set forth in TJNAF's Meeting and Conference Policy, Administrative Manual 104, and are responsible for ensuring that all participants understand and follow discussion restrictions to protect sensitive technology and information.

Meetings or conferences hosted by TJNAF that are determined to be public events will be prominently marked in all announcements, invitations, or promotional materials with the following statement:

> "This meeting or conference is a public event and as such all information to be presented or discussed must meet DOE standards for public release, and no

information will be presented or discussed that is proprietary or protected from release by statue, regulation, or DOE policy."

Once an event is approved, public-event organizers must advise foreign national participants attending without UFNA approval they must remain within the GAA boundaries during their visit when not escorted by a trained host or escort as detailed in paragraph 4.2 of this plan.

3.0 UFNA Requirements Implementation at TJNAF

In this section, *documentation*, *lawful immigration status*, *countries of risk*, *nationals of state sponsors of terrorism requests*, *indices checks*, and *access requirements and approval* will be addressed.

3.1. Documentation

Access Request

Except for the circumstances described in section 2.0 above, all foreign nationals requesting access to perform work or attend meetings and conferences at TJNAF; access to participate in TJNAF hosted virtual meetings and conferences requiring a registration; and access to TJNAF information systems where a user login and password is required must register an access request in the Electronic Access Registration System (EARS). Foreign nationals must provide sufficient documentation to verify their identity, authority to work, and lawful immigration status. The foreign national must provide the following documents and information to be verified by the immigration subject matter expert (SME):

- FACTS form (general biographical data and visit request information including country(ies) of affiliation, justification for access including specific activities or involvement and identification of the information or technology to be accessed, identification of the DOE program or sub-element and its mission advanced by the access and the proposed start and end dates). These forms are uploaded daily and must be entered *no later than* the start date of access.
- Curriculum Vitae. The CV (only required for those conducting research at TJNAF) must include education and work history since the age of 18 plus any science and technology specialties.
  - The history must accurately identify the current name and physical location (city and country) of each employer or academic institution and all degree/diplomas earned. There should not be any gaps in time over the past 10 years.
  - CVs should *not* contain personal identification numbers or other personal information.
- Institutional affiliation documentation. (This is a TJNAF local requirement.)
- Government-issued picture ID and U.S. Citizenship and Immigration Services documents. See 3.2 below.

When a foreign national submits a registration form, they certify that they have read and agree to the following terms and conditions (presented in Table 1 to draw attention to the critical elements):

Table 1 – Guest Certifications

Guest Certifications
The **terms and conditions** of access approval, including the requirement to notify their host of changes in name, and/or immigrant/non-immigrant status;
to **notify their host** of any civil or criminal problems that could affect their status and association with Jefferson Lab and/or DOE; and
that their **failure to provide** appropriate documentation, or providing fraudulent documentation, will result in suspension of their access approval, removal from the site, and possible cancellation of future access to Jefferson Lab.

When a registration form is forwarded to the host, the host must concur with the access, detail the scope of information or technologies to be accessed, including whether the foreign national will have access to sensitive subjects (list issued by the Cognizant Secretarial Office)—including restricted information/technologies identified in the Science and Technology (S&T) Risk Matrix—identify the physical area(s) to be accessed, and assign training requirements.

At the end of the form, the host certifies that they have read and agree to the following host responsibilities:

Table 2 – Host Certifications

Host Certifications
Ensure all requirements in the Electronic Access Registration System are completed prior to access.
Ensure that the foreign national, upon arrival on-site, reports to the Support Services Center (Bldg. 28) front desk for ID and immigration document verification.
Assign training, system, site and technology access that is appropriate for the scope of work.
Be aware of the day-to-day work activities of the foreign national and report any suspicious behavior or attempts to gain unauthorized access to the site, systems, or technologies.
Communicate the foreign national's obligations to report any change in name, immigration status, and any civil or criminal justice problems encountered during access.
Verify that site access credentials are collected and returned and that access to information systems is disabled upon completion of the access.
Assign a new host if at any point a host is unable to fulfill their duties for any reason, including absence from the lab—and have the new host report to Jefferson Lab Registration and International Services (JRIS).

Foreign Access Central Tracking System

The Foreign Access Central Tracking System (FACTS) is DOE's national database for unclassified foreign national access. The FACTS form and CV are uploaded into FACTS for both on-site and remote-access requests no later than the first day of access.

FACTS Database Access

The order specifies that access to FACTS is limited to U.S. citizens only. Further, a limited number of JSA employees in the Security and JRIS offices require access to FACTS to perform their processing and program oversight roles and responsibilities. For those employees assigned oversight and processing duties, the User Registration for a FACTS account is requested on the FACTS site at fnis.esportals.com/login.cfm.

Records

All foreign national access packages are marked Official Use Only and safeguarded in accordance with the Security Plan for Protection of Sensitive Information. The Security Office maintains the official FACTS records in a fireproof-safe, locked cabinet accessible only to authorized Security staff—or, electronically, in JList (Jefferson Lab Information System Toolkit) in the corresponding visit entry.

Retention

UFNA files where the information (including biographical, access information, reviews and approvals, close-out, and ID documentation) has been entered into FACTS can be destroyed one year after the end date of the access corresponding to the end of the fiscal year. All other files retained without potential for exposure to hazardous material may be destroyed five years after the end date of the access corresponding to the end of the fiscal year.

3.2. Lawful Immigration Status

Sufficient documentation of immigrant or nonimmigrant status, citizenship, and identity is required from all foreign nationals requesting access to TJNAF facilities, information, and technology—to verify their identity, authority to work, and lawful immigration status in the United States (including those that have received Delayed Action for Childhood Arrivals (DACA) status).

The following documents are collected as required for verification during the access registration process (expired documentation is not accepted):

- Government-issued picture identification
- Passport
- Visa or Legal Permanent Resident Alien Card (Green Card)
- Current U.S. Citizenship and Immigration Services documents

Remote access requests from foreign national guests located *outside* the United States require only the submission of a valid government-issued picture identification. Remote access requests for foreign national guests residing *within* the United States require the submission of a passport and U.S. Citizenship and Immigration Services documents.

UFNA End Date

The UFNA end date for foreign national guests may *not* exceed one year—*or* the end of their legal immigration status to be in the United States, whichever is shorter. At the end of an approved access period, foreign nationals can submit a registration request to extend their current access in accordance with the applicable Guest or Staff access policy. The request

will follow the same process as an original request; however, an addendum will be created in FACTS to extend the original request rather than create a new entry. Foreign national employee access may be for a maximum duration of four years—or the end of their legal immigration status to be in the United States, whichever is shorter.

To ensure compliance with the requirement that lawful immigration status be valid for the duration of the access, the JList Off-Site Date for foreign nationals on-site must correspond to the FACTS Desired End Date except for employees with Legal Permanent Resident status in the United States. Expiration emails are automatically generated based on the JList Off-Site Date, notifying the foreign national that their access will end on the given date—and requiring them to complete another access registration if continued access is required.

Information documenting the final status of access requests must be entered within 15 days after the last day of access. This includes the closeout status, closeout comments, and actual start and end dates for the access completed.

3.3. Nationals from a Country(ies) of Risk

The following applies to a foreign national born in, a citizen of, employed by, or represents a government, company, institution, or other organization based in a country identified as a country of risk. Contact the Security and Services Manager at (757) 269-7548 for country identification.

Access requests submitted by nationals from countries of risk to conduct research work under a facility User Agreement with TJNAF are exempt from the review requirements under CRD (Att. 1)(3)(g), including new facility User Agreements with institutions from a country of risk.

Access requests submitted by nationals from countries of risk to conduct research work without a facility User Agreement in place may not access areas identified as restricted in the S&T Risk Matrix without an exemption granted by the Under Secretary of Science or their designee (DOE Order 142.3B CRD(Att. 1)(3)(g)). All other access requests in areas not restricted in the S&T Risk Matrix can proceed with the normal review and approval process.

Upon receiving an access request where an exemption is required, the Local Approval Authority, in coordination with the host, TJNAF management, and the Thomas Jefferson Site Office's (TJSO) Officially Designated Federal Security Authority (ODFSA) will evaluate the access merits and benefits to the lab and DOE, and decide whether to proceed with the applicable approval process.

a. If the decision is not to proceed with the approval process, the Local Approval Authority denies the access request and notifies JRIS and host of the decision. Host is responsible for notifying the foreign national.

b. If the decision is to proceed with the applicable approval process, the following occurs:
    1. The Local Approval Authority collects all required documentation and information from the host and foreign national to provide a clear justification of why the access request benefits the U.S.

2. Local Approval Authority enters information into the Foreign Access Central Tracking System (FACTS) at least 45 days in prior to the requested start date to allow for the indices check to be completed, notifies DOE Counter Intelligence (CI) of the request for specialized enhanced vetting review with notification given to the TJSO.
3. Following the CI review results, the Local Approval Authority will submit the request package to the TJSO to initiate the approval process.
4. Once the ODFSA agrees to request the exemption, the request is submitted through the Office of Science, with a copy sent to the Federal Oversight Advisory Board (FOAB).
5. The Under Secretary of Science or their designee, in consultation with the Office of Intelligence and Counterintelligence, will make the final approval decision for these access requests.
6. Once a final decision is received, the Local Approval Authority notifies the host, TJNAF management, and JRIS. If the exemption is approved, the request will continue through the local approval process. The host notifies the foreign national of the decision.

If there is a need for a broad exemption for a specific category of access request (i.e., government-to-government agreements), the Security and Services Office will work through the TJSO to submit the exemption to the Under Secretary in consultation with the FOAB.

Foreign nationals with current access to TJNAF or its information systems are not subject to review for possible intersections between the S&T Risk Matrix and the performance of their research or lab duties until the time of their next access renewal. If upon access renewal a foreign national employee of JSA is assessed to have intersections with restricted areas of the S&T Risk Matrix, JSA assumes the exemption request will be granted under CRD (Att. 1)(3)(g)(1)(b).

3.4. Nationals from a State Sponsor of Terrorism (SST)

The following approval request process applies to a foreign national born in, a citizen of, employed by, or represents a government, company, institution, or other organization based in a country on the Department of State list of state sponsors of terrorism. Contact the Security and Services Manager at (757) 269-7548 for country identification.

Access requests for nationals from a SST who are not lawful permanent residents (LPRs) require approval from the ODFSA before a final approval determination can be requested from the Office of Science. Final approval authority is held by the Secretary of Energy who can only delegate their authority to the Deputy Secretary or Under Secretary of Science. The Under Secretary of Science, in consultation with the Office of Intelligence and Counterintelligence, will make the final approval decision for these access requests.

As soon as the information can be collected on a SST access request, the information shall be loaded into FACTS to start the indices check with notification sent to CI. An indices check or CI review (Note: CI consultations may not be used in lieu of indices checks until 60 days after requests are entered into FACTS) must be obtained before a SST package can be

forwarded to the Local Approval Authority.

Upon receiving the results of the indices check and the CI review, the Local Approval Authority will consult the host, management, and the ODFSA to determine whether to proceed with the request.

a. If the decision is not to proceed with the approval process, the Local Approval Authority denies the access request, makes closeout entry in FACTS, and notifies JRIS and host of the decision. Host is responsible for notifying the foreign national.

b. If the decision is to proceed with the applicable approval process, the following outlines the documentation required for the approval process:

- SST Template Processing Checklist
- Memo to the Under Secretary for Science
- SME Approvals
- FACTS printout
- Specific Security Plan
  - Current INS Documents
- Current Passport and Visa Documents
- CV
- Letters of Support (if readily available)
- Local Approval Signatures (from the lab and TJSO)

If approval is required from the Final Approval Authority, the Local Approval is entered into FACTS and notification sent to Nancy Day (Nancy.Day@science.doe.gov) or Mark Thornock (Mark.Thornock@science.doe.gov), who will process and forward the package for Headquarters Program Secretarial Office approval after all required documentation is entered in FACTS.

Note: *If an Office of Science approval is required, the process could take up to one year or more for a decision. If the SST national is a LPR eligible for local site approval, the process could take 30 days or more for a decision*.

Specific security plans will be developed to protect sensitive information/technology as necessary pursuant to DOE approval guidance. The Local Approval Authority, CI, and Cyber Security develop these plans.

Access to TJNAF campus buildings, TJNAF offices and labs in the Applied Research Center, and the Accelerator Site will only be granted to nationals of state sponsors of terrorism once approval is received and communicated through the TJSO. The Local Approval Authority will then notify the host of an access approval or if a determination was made to cease a request.

3.5. Indices Checks

As detailed in Table 3 under paragraph 3.6, indices checks are required for all nationals from a SST, as well as sensitive country nationals and any requests involving sensitive subjects. The Office of Intelligence and Counterintelligence coordinates such checks, which are

automatically initiated when a request is submitted in FACTS. Checks are valid for a period of two years and renewal requests are automatically generated in FACTS prior to the expiration date.

Only access requests for sensitive country nationals working with sensitive subjects and SST requests require an indices check be completed before an approval determination. For all other requests requiring indices checks, the check does not have to be completed by the start date. However, the indices check for a SST national *must* be completed prior to submittal of a request to the approval authority.

3.6. Access Requirements and Approvals

Following the SME reviews discussed in 4.2 below, all foreign national access to TJNAF's site, information, and technologies must be approved by either the Local Approval or Final Approval Authority according to Table 3. Access approvals are subject to validation and verification of the information submitted during registration. The local approvals are documented in FACTS. The following requirements apply:

Table 3 – TJNAF UFNA Requirements

	FACTS Documentation and Timeliness Requirements	Indices Checks and Completion Requirements	Approval Authority
Non-sensitive Country Nationals (No Sensitive Subjects)	No later than start date	Not required	Local Approval Authority
Sensitive Country Nationals (No Sensitive Subjects)	No later than start date	Does not have to be completed by start date	Local Approval Authority
Sensitive Subjects, Non-sensitive Country Nationals	No later than start date	Does not have to be completed by start date	Local Approval Authority
Sensitive Subjects, Sensitive Country Nationals	Recommended to be entered 45 days prior to start date	Must be completed prior to start of access	Local Approval Authority

Nationals of State Sponsor of Terrorism	In time to obtain final approval	Must be completed before approval determination	- LPRs – Local Approval Authority
			- All others:
			  - Initial – Final Approval Authority
			  - Subsequent – Local Approval Authority

The approval authority shall take the following into consideration before granting approval:

- All information from the SME review process as well as the potential impacts on site operations to determine associated access risks, order compliance and mission benefits.
- Any identified risk to the government associated with the access granted must be appropriately evaluated and mitigated—and is needed to support DOE program objectives and/or U.S. national interests.
- Legal and policy-related terms and conditions associated with the requested access must be met before approval (i.e., visa status conditions and requirements, right-to-work requirements, and international agreements).

4.0 UFNA Responsibilities at TJNAF

These responsibilities reside in the TJSO and JSA, explained as follows.

4.1. Thomas Jefferson Site Office

Approval authority and accountability for foreign national access to TJNAF and associated information or technology is the TJSO Manager. Line management accountability flows from the TJSO to the Director. If the Director is not a U.S. citizen, the TJSO will assign approval authority to another management official. The TJSO Manager is the Officially Designated Federal Security Authority (ODFSA) and is the Local Federal Signature Authority for SST access. The TJSO Security Manager is the Officially Designated Security Authority assigned oversight responsibility for the UFNA program.

Assignment of Local Approval Authority

The ODFSA has delegated the approval authority to the Lab Director. The Lab Director is accountable for all access approval decisions made by himself or those to whom he delegated approval authority. The Lab Director may reassign approval authority in writing to other U.S. citizen JSA employees. Further reassignment is not allowed. All site approval authorities are defined in this Program Plan.

The Lab Director delegated Local Approval Authority to the Security and Services Manager and the Chief Operating Officer in January 2019.

4.2. Jefferson Science Associates

The Security and Services Office, Facilities Management Division, is responsible for managing the UFNA program.

Subject Matter Expert Review

Each access request undergoes the following subject matter expert reviews: Immigration, Export Control (including export license determination) and Technology Transfer. Additionally, an SST national request will include a Cyber Security review plus a Counterintelligence SME review—to include a completed indices check.

TJNAF's UFNA Program SMEs and review officials are designated by duty position and

function. The following positions (shown at Table 4) are designated SMEs for the UFNA program and participate in the standard SME review for all requests. These experts are defined in the CRD (Att. 2)(32) and listed as the UFNA Contacts and Designated Officials.

Table 4 – TJNAF Subject Matter Experts

Tasks	JSA Duty Position
Immigration	Visa & Immigration Administrator
Export Control/Site Security	Security and Services Manager
Counterintelligence*	DOE Counterintelligence Officer
Technology Transfer	Security and Services Manager
Cyber Security*	Cyber Security Manager

*Only review access packages for SST national and S&T Risk Matrix restrictions.

Reviews allow SMEs to assess each request and identify potential impacts that the approval authority should consider while making the approval determination. In addition, the export control and technology transfer reviews must document if an export license is required. The SME reviews are documented in FACTS.

UFNA Program Contacts and Designees

TJNAF's UFNA Program Contacts List (CRD (Att. 1)(4)(a)(3)) is approved by the Lab Director and the DOE TJSO Manager or their designees, with copies provided to the DOE TJSO, lead program Secretarial Officer (LPSO), and the Office of Health, Safety and Security. The list must be updated whenever a change in personnel takes place.

Hosts

Hosts are responsible for the conduct and activities associated with the successful accomplishment of the activity. If a host is not designated when a foreign national submits a guest access registration, the JRIS appoints one based on the description of work that the foreign national includes on the registration form. When a registration is forwarded to the host, they must complete the following:

- concur with the access request
- detail the scope of work
- identify if sensitive subjects including S&T Risk Matrix restricted technology areas will be discussed
- assign training requirements
- assign building access requirements (identification of areas to be accessed)
- assign an escort as required

At the end of the host form, the host certifies that they have read and agree to their foreign national host responsibilities detailed in Section 3.1, Table 2 – Host Certifications.

Only DOE or JSA employees can host or escort foreign nationals. Foreign nationals of countries designated as state sponsors of terrorism may not host other foreign nationals. Hosts must ensure the foreign national's compliance with all requirements for access approval, including timely, complete, and accurate information for FACTS; security plan (if

required), SME reviews, program sponsorship (such as exchange visitor programs); and provide notification to workers regarding requirements as appropriate.

In addition to the responsibilities above, hosts are also accountable for the following:

- Complete, annually, TJNAF's GEN 006, Hosting Foreign National Access at Jefferson Lab. JSA and DOE staff may not serve as a host until this training is completed.
- Provide the following information to the foreign national that the employee is responsible for hosting:
  - Hosts are the foreign national's POC for the access.
  - The terms and conditions of access approval, including restrictions and requirements to notify the host of changes in name, immigrant/nonimmigrant status, and other information as required.
  - The requirement to notify the responsible host of any civil or criminal problems that could affect their status and association with DOE.
  - Failure to provide appropriate documentation when required—or providing fraudulent documentation—will result in suspension of access approval, removal from the site, and possible cancellation of future access.

Escorting Foreign National Guests

To ensure there is no unauthorized access by foreign nationals, the following escort requirements are in place:

- Only host-trained (GEN 006) JSA and DOE staff may serve as escorts for foreign nationals (other than construction subcontractors, addressed below).
- Foreign national guests without badged access must be escorted by their host and/or JSA staff designee (who must have host training) at all times when outside a GAA.
- Foreign National Delivery Drivers must report to Shipping and Receiving. If necessary, said personnel will escort the driver to the location of the delivery and remain with the driver until the driver's departure from TJNAF premises.
- Construction subcontractor deliveries can be escorted by a badged construction subcontractor *from entrance to exit*. All other construction subcontractors must be registered and badged.

5.0 Definitions

Access Request – Seeking permission to enter TJNAF and/or use TJNAF Information or technologies requiring registration in the Electronic Access Request System.

Country of Risk - Any foreign country determined to be of risk, following consideration of, but not limited to, the Office of the Director of National Intelligence World Wide Threat Assessment and the National Counterintelligence Strategy of the United States of America, by the Under Secretary for Science in consultation with the Under Secretary of Energy; the Under Secretary for Nuclear Security; and the Office of Intelligence and Counterintelligence.

Curriculum Vitae (CV) - A detailed document highlighting professional and academic history. A CV must include any education/employment history. There should be no lapses in time. CVs include extensive information on academic background, including teaching experience, degrees, research, awards, publications, presentations, and other achievements. In the absence of a CV, a resume may be used.

Dual Citizen - An individual who is a citizen of more than one country.

Export Controlled Information – Any information or material that cannot be released to foreign nationals or representatives of a foreign entity, without first obtaining authorization or license from the Department of State for items controlled by the International Traffic in Arms Regulations (ITAR), or the Department of Commerce—for items controlled by the Export Administration Regulations (EAR). Export-controlled information is Controlled Unclassified Information (CUI) Specified and marked accordingly.

Final Approval Authority – Held by the Secretary of Energy and can only be assigned to the Deputy Secretary, Under Secretary for Nuclear Security/Administrator of the National Nuclear Security Administration, Under Secretary of Energy, or Under Secretary for Science. The Deputy Secretary or appropriate Under Secretary, in consultation with the Office of Intelligence and Counterintelligence, will make the final approval determination.

Foreign National – A person without U.S. citizenship or nationality (may include a stateless person).

Fundamental Research – Basic and applied research in science and engineering where the resulting information is ordinarily published and shared broadly within the scientific community. A full discussion of the issue of fundamental research is provided in section 734.8 of the Export Administration Regulations and National Security Decision Directive 189, “National Policy on the Transfer of Scientific, Technical, and Engineering Information.”

General Access Area – A type of security area established to allow access to certain areas with minimum security requirements as determined by the cognizant security authority. These designated areas are accessible to all personnel including the public.

Host – The JSA employee or DOE TJSO employee qualified to prevent access to sensitive information, technologies, or equipment and responsible for the activities associated with foreign national access.

Indices Check – A procedure whereby a request is made to appropriate U.S. Government agencies to determine whether information exists on a particular foreign national. Indices checks are valid for a period of two years from the indices’ completion date, as documented in the Foreign Access Control Tracking System by the Office of Intelligence and Counterintelligence.

Information – DOE or TJNAF information of a programmatic, scientific, or technical nature, regardless of format or medium on which it is recorded, created, or possessed by the Government of a Contractor.

Lawful Permanent Resident (LPR) – One who has the right to reside permanently and work in the United States. Unlike a U.S. citizen, however, an LPR is not permitted by states to vote in national elections and can be deported if, for example, convicted of certain crimes. An LPR may

also be known as a permanent resident alien or Green Card Holder.

Local Approval Authority – The accountable DOE and JSA employee(s), designated in writing by the Lab Director, responsible for review and approval of all access requests to TJNAF's site, program, information, or technology.

National of a Country of Risk – A foreign national who was born in, is a citizen of, is employed by, or represents a government, company, institution, or other organization based in a country identified as a Country of Risk.

National of a State Sponsor of Terrorism – A foreign national who was born in, is a citizen of, is employed by, or represents a government, company, institution, or other organization based in a country on the Department of State list of State Sponsors of Terrorism.

National Security – The national defense and foreign relations of the United States.

Non-Sensitive Country National – A foreign national who was born in, is a citizen of, is employed by, or represents a government, company, organization, or institution that is located in a country not on the sensitive country list and not a State Sponsor of Terrorism as identified by the Department of State.

Personal Visit – A personal visit does not include access to DOE or TJNAF information or technology. Examples may include lunches with friends or relatives, retirement celebrations, or other social events.

Property Protection Area – A type of security area having defined boundaries and access controls for the protection of DOE and TJNAF property.

Proprietary Information – Information that contains trade secrets or commercial or financial information that is privileged or controlled, and may only include information described as follows:

- Has been held in confidence by its owner.
- Is of a type customarily held in confidence by its owner.
- Has not been transmitted by the transmitting party or entities (including the receiving party), except on the basis that it be held in confidence.
- Is not otherwise available to the receiving party from another source without restriction on its further dissemination.

Property Protection Area – A type of security area having defined boundaries and access controls for the protection of Departmental or TJNAF property.

Public Event – Public events are those that include only information that is not protected by statute, regulation, or DOE policy, *and* is determined to be releasable to the general public, are held in locations that are accessible to the general public, and are available for attendance by the general public.

Remote Access – Approved computer account access provided to registered and trained persons collaborating offsite with TJNAF at for-profit organizations or institutions of research or higher learning.

Research – Systematic investigation, including research, development, testing and evaluation designed to develop, expand or contribute to general knowledge.

Science and Technology (S&T) Risk Matrix – Critical emerging research and technologies that require protection and that do not otherwise have control mechanisms (i.e., classified information, International Traffic in Arms Regulations, export controls). The S&T Risk Matrix is intended to highlight areas of emerging and potential concern associated with economic and/or intellectual competitiveness and not to overlap or supersede existing controls associated with national security or commerce restrictions.

Sensitive Country List – A list of countries to which particular consideration is given for policy reasons during the DOE internal review and approval process for access by foreign nationals. Countries may appear on the list for national security, nuclear nonproliferation, or terrorism support reasons.

Sensitive Country National – A foreign national who was born in, is a citizen of, or is employed by a government, employer, institution or organization of sensitive country.

Sensitive Subjects – Unclassified subjects/topics identified in existing Federal Regulations governing export control as well those identified by the DOE as unique to its work, which involve information, activities, and/or technologies that are relevant to national and economic security. This includes items identified in the research areas determined to be restricted in the current S&T Risk Matrix and items identified as Controlled Unclassified Information (CUI) Specified.

Specialized Enhanced Vetting – Vetting required to support S&T Risk Matrix exemption approval determination to be conducted by the Office of Intelligence and Counterintelligence based on the individual's background. The S&T Risk Matrix exemption request, including the completed supplemental questionnaire, is utilized to perform an enhanced background check with Intelligence Community partners.

State Sponsors of Terrorism (SST) – Countries identified by the Department of State as sponsors of groups and/or activities that support terrorism or terrorism activities and are on the List of State Sponsors of Terrorism. TJNAF will use the prevailing list posted at the DOE FACTS website. TJNAF Security and Services will provide the prevailing list to those needing access for official purposes.

Subject Matter Expert – An individual who is knowledgeable about the professional standards, requirements, and practices used within the discipline he/she represents (i.e., security, export control, technology transfer, counterintelligence, or intelligence.)

Technology – Technology is derived from basic or applied research, development, engineering, technological demonstration, economic and social research, or scientific inquiry into phenomena or technology applications. It included the use and application of scientific equipment, may be recorded or spoken, may be represented in a medium for storage for storage of communication, and may be contained in computer software with scientific and technical applications.

Third-Party Events – Events, activities that a DOE site hosts that are not directly in support of the DOE mission; does not include information that is protected by statute, regulation, or DOE policy and is determined to be releasable to the general public.