Jefferson Lab

Personnel Security Program Plan

5 June 2023

U.S. DEPARTMENT OF ENERGY

JSA

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

Submission and Approval

Submitted by:

Brian Hanlon, Security and Services Manager
Jefferson Science Associates, LLC
TJNAF Facilities Management and Logistics Division

15 OCT. 2019
Date

Reviewed by:

Rusty Sprouse, Facilities Management and Logistics Manager
Jefferson Science Associates, LLC
TJNAF Facilities Management and Logistics Division

16 Oct 19
Date

Approved by:

Micha ;r, Chief Operating Officer
Jefferson Science Associates, LLC
TJNAF COO Division

17 OCTOBER 2019
Date

Richard D. Korynta, Security Program Manager
Department of Energy, TJNAF Site Office

10-18-19
Date

Revision History

Revision History		
Rev.	**Date**	**Reason**
0	15 October 2019	Original
1	July 2020	Administrative Change to include omitted requirements
2	5 June 2023	Corrected Security Plan Appendix Numbering

Table of Contents

TABLES

ATTACHMENTS

Abbreviations and Acronyms

AR	Administrative Review
CFR	Code of Federal Regulations
CIRC	Computer Incident Response Center
CNSI	Confidential National Security Information
CFRD	Confidential Formerly Restricted Data
CRD	Confidential Restricted Data
CSO	Cognizant Security Office
DOE	Department of Energy
FSO	Facility Security Officer
IOSC	Incident of Security Concern
MI	Management Interest
ODFSA	Officially Designated Federal Security Authority
TJSO	Officially Designated Security Authority
ORO	Oak Ridge Office Consolidated Support Center
PI	Procedural Interest
PPM	Program Planning Management
SAP	Special Access Program
SCI	Sensitive Compartmented Information
SFRD	Secret Formerly Restricted Data
SNSI	Secret National Security Information
SNM	Special Nuclear Material
SRD	Secret Restricted Data
SSIMS	Safeguards and Security Information Management System
TFRD	Top Secret Formerly Restricted Data
TJNAF	Thomas Jefferson National Accelerator Facility
TJSO	Thomas Jefferson Site Office
TNSI	Top Secret National Security Information
TSRD	Top Secret Restricted Data
U.S.C.	U.S. Code

Personnel Security Program Plan

1. Purpose

This plan implements a Personnel Security Program required by the Personnel Security, Contractor Requirements Document, DOE Order 472.2, Change 2. The provisions of JSA's contract with the Department of Energy (DOE) does not authorize Thomas Jefferson National Accelerator Facility (TJNAF) to receive, store, transmit, or originate classified information. However, a small number of employees hold clearances initiated through JSA to allow them to receive classified briefings from DOE and other agencies that may impact the security and safety of TJNAF. This plan sets forth the personnel security program management and work practices to support JSA's Personnel Security Program.

References include the following Department of Energy orders:

- DOE O 472.2, CRD, Personnel Security
- DOE O 470.4B, CRD, Safeguards and Security Program
- DOE O 475.1, CRD, Counterintelligence Program

2. General Requirements for Security Clearances

Before an employee is processed for a security clearance, proper documentation must be in place. Jefferson Science Associates' must possess a Department of Energy-issued facility clearance and a contract requiring the proper security clearance for designated personnel. The JSA facility security officer (FSO) and Thomas Jefferson Site Office's officially designated federal security authority (TJSO ODFSA) will verify the necessary background documentation is in place before submission to the Consolidated Support Center, Cognizant Personnel Security Office-Oak Ridge (ORO). The FSO coordinates all security clearance matters for existing JSA clearance holders and new applicants.

The following details further the general requirements for obtaining security clearances:

- Security clearances for JSA personnel must only be requested when required and maintained at the minimum number necessary to ensure operational efficiency. The number of assigned Jefferson Lab positions necessitating a security clearance is limited because the job requires actual or potential access to classified material.

- A security clearance should not be requested for any of the following reasons cited in DOE O 472.2, CRD, Personnel Security, Attachment 1 paragraph 1 (c):

    - To avoid the use of access controls or physical barriers to distinguish perimeters among security areas or between security and open areas;
    - Alleviate responsibilities for escorting persons without security clearances within a controlled area.

- Alleviate individual or management responsibilities for properly protecting classified information or SNM or controlling dissemination of classified information or SNM on a need-to-know basis;
- Determine an individual's fitness for employment with the contractor;
- Establish a pool of contractor employees with pre-existing security clearances;
- Accommodate an individual's personal convenience, expedience, gain or advantage;
- Anticipate unspecified classified work.

- The U.S. Government determines whether a person is eligible for access to classified matter – that is, to obtain a security clearance.

- For a JSA employee to obtain a security clearance, a federal investigative agency must investigate that person's background.

- Individual access to classified information is only authorized after DOE notification that a clearance has been granted.

- If a clearance is required for DOE and another Federal agency, JSA will submit the request for the highest security clearance necessary, and rely upon reciprocity for lower clearances.

- If a non-U.S. citizen possesses unique or unusual skills or expertise that is urgently needed to support a specific DOE mission involving access to classified information, and a qualified U.S. citizen eligible for such access is not available, JSA can submit non-U.S. citizens for consideration of a Limited Access Authorization (LAA). Reference chapter 6 below.

3. Types, Levels and Categories of Security Clearances

Five types of security clearances exist at DOE: Q, L, top secret, secret, and confidential. The work that an employee will perform, and the terms of the contract, determine that employee's security clearance. JSA personnel requiring a clearance are issued Q or L clearances, as there is, as of this writing, no classified material at TJNAF.

Security clearances are classified into three levels:

Confidential: The unauthorized disclosure of confidential information or material can cause measurable damage to national security. This level is reinvestigated every 15 years.

Secret: The unauthorized disclosure of secret information can cause serious damage to national security. This level is reinvestigated every 10 years.

Top Secret: The unauthorized disclosure of TS information or material can cause grave damage to national security. This level is reinvestigated every 5 years.

In addition, three categories of classified matter are identified: Restricted Data, Formerly Restricted Data, and National Security Information. The employee must have a security clearance consistent with their assignment.

The types of DOE clearances and the categories of classified matter they correlate with are reflected in the table below:

Q	Top Secret	L	Secret	Confidential
TSRD				
SRD				
CRD		CRD		
SNM CAT I - III		SNM CAT II & III		
TSNSI	TSNSI			
SNSI	SNSI	SNSI	SNSI	
CNSI	CNSI	CNSI	CNSI	CNSI
TSFRD	TSFRD			
SFRD	SFRD	SFRD	SFRD	
CFRD	CFRD	CFRD	CFRD	CFRD

Table 1 – Clearance Levels and Classified Matter

4. Security Clearance Eligibility

Only JSA employees that are U.S. citizens 18 years and older can apply for a security clearance. JSA does not have any subcontracts requiring access to Restricted Data (RD), Special Nuclear Material (SNM) or other classified information or matter; therefore, Subcontractors are not eligible to receive a clearance through JSA.

Key Management Personnel – Such personnel are top JSA and Southeastern University Research Association officials performing contractual/oversite work of the contract, which may include classified work for DOE. If access to classified information is required, key management personnel must have a DOE security clearance commensurate to the level of the contract, according to the DOE Foreign Ownership, Control, or Influence Program.

The following Jefferson Lab key management personnel positions are eligible to be cleared for "Q" level security clearances:

Laboratory Director	Deputy Director, Science & Technology
Chief Operating Officer	JSA Board of Directors Chairman
Chief Information Officer (CIO)	Chief Financial Officer (CFO)
Information Systems Security Officer (ISSO)	Information Systems Security Manager (ISSM)
	Facility Security Officer (FSO)

Table 2 – JSA Positions Requiring a "Q"-Level Clearance

Unpaid Consultants - When processing a security clearance request for an individual who will be providing services as an unpaid consultant, the FSO must ensure that an adequate justification is included in the security-clearance-request package. Also, the package must include a copy of the consultant's "Affirmation Agreement/Statement of Work."

5. The Clearance Process In Detail

New and Existing Employees – New or existing JSA employees and others designated as requiring security clearances must coordinate with the facility security officer to prepare the required documentation. The FSO coordinates with the TJSO to obtain the required signatures and submit the security clearance request package.

Prior to starting the clearance process, applicants will be given the "Obligations" sheet reminding them of their responsibility to (1) truthfully provide all information requested for personnel security purposes, and (2) to report situations/incidents found in Table 3 which summarizes the information found in DOE O 472.2, Attachment 1, Paragraph 7.b.3 and Attachment 4 (i.e. any criminal arrests, bankruptcy filings, changes in citizenship, etc…), see Attachment 2.

Individuals must have the opportunity to complete and submit all forms, or other data collections required during the clearance process, in private. The FSO or other knowledgeable personnel that JSA specifically designates to review such forms, will assist if required. Processing an application for a security clearance involves several steps and multiple officials. It is recommended that individuals maintain copies of their completed security forms for personal records.

The following explains the clearance process in both detail and sequence, from the TJSO's responsibilities to that of the JSA employee-applicant for clearance.

1. Determining Sponsorship – TJSO must sponsor all applicants for security clearance. The TJSO, in coordination with the FSO, provides all clearance related actions, including reinvestigations, completion of security refresher briefings, etc.

2. Obtaining Documentation from the Applicant – The FSO must obtain the necessary information from the employee to prepare the required application documentation, including the following:

    - DOE F 473.3, Clearance Access Request;
    - DOE F 5631.18, Security Acknowledgement;
    - DOE F 206.4, Information Sheet for Sponsorship of Homeland Security Presidential Directive – 12 Credential;
    - Letter of Justification (see #4 below);
    - Credit Release Form (Fair Credit Reporting Act 15 USC 1681 compliant);

- Negative results from drug test (see #5 below);
- Complete e-QIP submission; and
- FD 258, Applicant Fingerprint Chart or fingerprints taken electronically via an approved capture method.

3. Pre-employment and Pre-processing Requirements – Those persons requiring a security clearance must provide evidence of citizenship and verify such evidence to the FSO and/or TJSO. Acceptable evidence of U.S. citizenship consists of the following:

<table>
<tr><th>Born within the United States</th><th>Born abroad to a US Citizen</th><th>Naturalized Citizen</th></tr>
<tr><td>United States Passport
(current or expired)</td><td>Certificate of Naturalization
(Form N-560 or N-561)</td><td rowspan="5">Certificate of Naturalization
(Form N-550 or N-570)</td></tr>
<tr><td rowspan="3">Birth Certificate:
• Filed shortly after birth
• Certified
• Registrar’s signature
• Contain registrar’s seal, Raised, impressed or multicolored seal (Exception: the state or other jurisdiction does not issue seals as a matter of policy)</td><td>Consular Report of Birth Abroad
(State Department Form FS-240)</td></tr>
<tr><td>Certificate of Birth (Form FS-545 or DS-1350)</td></tr>
<tr><td>Record of Military Processing Armed Forces of the U.S. (DD Form 1966), provided it reflects U.S. citizenship</td></tr>
<tr><td>Delay birth certificate is acceptable when accompanied with the following secondary evidence; either original or certified:
• Baptismal records
• Hospital birth records
• Affidavits by person with personal knowledge of birth</td><td rowspan="2">United States Passport
(current or expired)</td></tr>
<tr><td>Other documentary evidence:
• Early Census
• School records
• Family records
• Newspaper files
• Insurance records</td><td></td></tr>
</table>

Table 3 – Evidence of U.S. Citizenship

4. The FSO will be responsible for creating and submitting to the TJSO the DOE F 473.3, Clearance Access Request (Attachment 3) justifying the request for security clearance. The justification must detail the following:
    - Full name of the individual;
    - Individual’s Social Security Number, and date and place of birth;

- Individual's status (Contractor employee);
- Contractor Name;
- The DOE contract or subcontractor number under which the security clearance is being requested;
- Primary Program code – SC;
- Facility Code – 307;
- Level of security clearance required, i.e. Top Secret, Secret, Confidential, Q or L;
- A detailed description (without revealing classified information) as to why the individual requires access. The description must include a full explanation of the information to be accessed, how often the access is needed, and for what programs/projects the information is needed.
- Full name and title and telephone number of the requestor; and
- Signature of the requestor.
- Whether or not the individual holds or previously held a security clearance issued by DOE or another federal agency.
- Verification of the individual's evidence of citizenship.
- Information regarding contractor reviews, if the TJSO requires it.

All completed security forms and related materials will be reviewed by designated JSA employees authorized to review the information solely for its adequacy and completeness prior to their submission to DOE.

The FSO will maintain records and documents associated with the processing and maintenance of all designated persons issued a security clearance, as follows:

- Records to be maintained will include documents showing, by contract numbers, all persons granted security clearances – including the employee's name and the date the security clearance was granted.
- Copies of correspondence to and from DOE to be maintained include the request for security clearance, notification that security clearance action was effected, security clearance termination, and administrative withdrawal action.

The records must be maintained for a period of two years after the individual's security clearance is terminated. All security records are stored and protected in a locked fire proof safe located in the FSO's uniquely keyed office. The FSO is the sole key holder to the storage safe.

5. Drug Testing – JSA personnel applying for a new security clearance must undergo a urinalysis drug screening for the use of illegal substances. DOE will not process a request

for a security clearance from an applicant who tested positive for illegal drugs.

The FSO will coordinate with the applicant and medical services to schedule a drug test. Medical services will provide the results to the FSO to be included in the security-clearance-access request package. Drug test results must be dated within 60 days of the date of the security clearance request.

Results of JSA's drug screening are reported in one of two ways: an attached copy of the medical-laboratory report showing the results of the drug test, or a letter attesting to the date, location and results.

6. Preparing a Request for a Security Clearance – The DOE F 473.3, Clearance Access Request, is the official request for the ORO to process the security clearance application. Once the applicant signs all documents and the pre-employment drug test results have been documented, all forms are assembled and attached to the DOE F 473.3.

   The FSO then submits it to the TJSO for processing and routing to the ORO. The TJSO must ensure the applicant's contract is registered in the SSIMS before signing the DOE F 473.3 and routing.

   The FSO, in coordination with the TJSO, must provide a satisfactory justification statement outlining the need for the security clearance. The justification must specify the highest classification level and category of matter to be accessed, and detail the duties requiring access at that level. It must also indicate whether the individual holds or has held a security clearance issued by DOE or any other federal agency.
   Requests must include the following:

   - Cover letter or form DOE F 473.3, Clearance Access Request.
   - Verification of the individual's evidence of U.S. citizenship, as detailed in paragraph 3 above.
   - The JSA contract number under which the security clearance is being requested.
   - Information regarding contractor reviews, pursuant to 48 C.F.R. 952.204-2(h)(2)(vi) [the DEAR Clause], if required by the ORO.
   - Negative results of the drug test.
   - A complete e-QIP submission that indicates no illegal use of a controlled substance for at least 12 months preceding the date of the individual's signature.
   - An FD 258, Applicant Fingerprint Chart, or fingerprints taken electronically via an approved capture method (e.g., at a General Services Administration-provided HSPD-12 enrollment center), when available. (Note: This is not required if a previous investigation included a classifiable fingerprint search by the FBI.)
   - DOE F 5631.18, Security Acknowledgement.

- A completed fair-credit-reporting-disclosure authorization, compliant with the Fair Credit Reporting Act, codified at 15 U.S.C. s1681 et seq. and approved for the Lab Director's use. (Note: Once obtained, DOE may use this authorization to conduct credit checks directly with consumer agencies as part of its personnel security program.)

7. Sponsorship in USAccess – The TJSO coordinates with the information technology security manager to sponsor and enroll the applicant into USAccess. The applicant must enroll in USAccess to have their fingerprints captured.

8. ORO Review of Documentation Submitted – The ORO reviews the documents to verify they are complete. If the request is deficient, the ORO advises the TJSO and FSO of the necessary corrections. When the documents are complete, the ORO emails them to the TJSO, who then initiates the applicant into e-QIP using the information contained in their application.

9. Background Investigation – Once the e-QIP process is completed, the applicant's information is automatically forwarded to the Defense Counterintelligence and Security Agency (www.dcsa.mil). The FSO shall assist with investigations by: 1) ensuring applicants are available for the interviews, and 2) ensuring that other employees are available to provide background information, if necessary. A completed background investigation is returned to the ORO.

10. Deficient Requests – If a security clearance request is deemed deficient by the ORO, the FSO will attempt to satisfactorily correct the noted deficiencies and return the package to ORO within 30 days. If circumstances prevent a timely resolution, the FSO shall communicate justification for the delay to the ORO.

11. Grant of Security Clearance – The ORO adjudicates the applicant's investigative report based upon Security Executive Agent Directive 4, National Security Adjudicative Guidelines, and 10 CFR 710. If a favorable determination is made, a security clearance determination will be granted and entered into the DOE Central Personnel Clearance Index. The ORO will email the official notification of the clearance grant.

    ORO cannot approve applicants with unresolved security concerns, as identified by 10 CFR 710.8 and the Adjudicative Guidelines. Instead, the application must be processed through the Administrative Review procedures contained in 10 CFR 710, as described in the subsection below.

12. Completion of Standard Form 312, Classified Information Nondisclosure Agreement The FSO or TJSO will have the applicant complete a Comprehensive Security Briefing, which describes the applicant's responsibilities for protecting classified information. The TJSO will witness and accept the Agreement. The FSO will retain the original SF-312 while the cleared individual is employed by JSA. The SF-312s retained will not be stored with personnel security files. They must be retained in a file system from which they can be expeditiously retrieved if the U.S. government seeks information or subsequent

employers require confirmation of execution. Original SF-312s retained by the FSO must be sent to ORO upon the termination of employment.

6. Limited Access Authorization

Limited Access Authorizations (LAA) are available for non- U.S. citizens who have not been cleared by any foreign government. Foreign nationals who have been investigated and granted the equivalent of a security clearance by a foreign government may be granted access to classified information at DOE via the passing of a security assurance by the foreign government to DOE in accordance with DOE O 470.4B.

A non-U.S. citizen, who possesses a special expertise, may be granted limited access to classified information for specific programs, projects, or contracts when there is a compelling reason to further a DOE mission. They will only be eligible for access to a level of classified information as the United States Government has determined is releasable to the country of citizenship of the individual as determined by the Director and the DOE Office of General Counsel.

A Limited Access Request is initiated by the *Program Secretarial Office* with jurisdiction over the information to be released by submitting a detailed request, including a justification, for the desired LAA to the ORO. The ORO will interview the Non-U.S. citizen to determine:

- The nature and extent of the individual's contacts and continuing associations with persons outside of the United States (including family members);
- The degree to which the individual exercises his or her foreign citizenship;
- Whether the individual or any associates (to include family members) are or have been affiliated with any foreign government; and
- The degree to which it is likely that the required background investigation can be conducted on the individual.

Following the interview the ORO will have DOE counterintelligence complete a preliminary CI-focused risk assessment. The requesting *Program Secretarial Office* will be notified if the assessment reveals that it would not be feasible to continue with the LAA process. The results of the interview, risk assessment, and other relevant information will be forwarded to the Director, Office of Departmental Personnel Security by the ORO if the results of the assessment warrant continued processing.

The decision to proceed with a background investigation or to cease the process is held with the Director. If the Director determines not to proceed, the ORO and the applicable Program Secretarial Office will be notified of the decision. If the Director decides to continue processing the LAA request, the Director will notify the ORO to start processing the background investigation for the individual. The background investigation will be processed in accordance with investigative and adjudicative procedures set forth in DOE Order 472.2, Personnel Security.

Once an adjudicative determination has been attained, a formal comprehensive CI-focused risk assessment will be initiated by the ORO. The results of the adjudication and the risk assessment

is then forwarded to the Director for concurrence. The Director will then concur and grant the LAA. If the Director does not concur, the ORO and the *applicable Program Secretarial Office* are notified. The Director's determination is final. A denial is not subject to review under the procedures set forth in 10 CFR 710.

The ORO will review all LAAs annually to ensure they are still needed following an annual re-justification by the *Program Secretarial Office* who initially requested the LAA. Annual re-concurrence of the Director is not needed as long as the ORO believes an individual meets the requirements of the LAA. Reinvestigations are conducted at intervals established by national policy for individuals holding Top Secret security clearances.

Once the individual is no longer employed by JSA or otherwise no longer requires the access for which the LAA was granted, or at the direction of the Director, the LAA must be administratively withdrawn by the ORO. If an individual no longer satisfies the eligibility requirements for an LAA, the LAA must be immediately revoked. An LAA may also be revoked at the direction of the Director. The revocations are not subject to administrative review procedures set forth in 10 CFR 710.

A non-U.S. citizen granted an LAA may not access SNM or to any of the following types of classified information:

- Top Secret, Top Secret CRYPTO, RD, FRD or Special Access Program (SAP) information.
- Information that has not been determined by a U.S. Government Designated Disclosure Authority to be releasable to the country of which the individual is a citizen.
- COMSEC information.
- SCI or Intelligence information.
- North Atlantic Treaty Organization (NATO) Information. A national of a NATO member nation may be authorized access to NATO information provided that a NATO Security Clearance Certificate is obtained by DOE from the individual's home country and such access is limited to performance on a specific NATO contract.
- Information for which foreign disclosure has been prohibited in whole or in part (identified as NOFORN).
- Classified information provided to the U.S. Government by a third party government and information furnished in confidence to the U.S. Government by a third party government.

7. Reciprocity

Reciprocity may be requested when the applicant currently holds a security clearance granted by another federal agency, or has had a favorably adjudicated investigation within the last 2 years, making them eligible for a security clearance. The ORO will attempt verification of the applicant's clearance through national databases, or directly from the adjudicating agency. When

a discrepancy exists in determining clearance eligibility, the five business day suspense to reciprocally accept another agency's background investigation does not apply.

An applicant who formerly held a security clearance at another federal agency, or had a favorably adjudicated background investigation that meets or exceeds the level of security clearance currently required, may be eligible to have a DOE security clearance granted through re-instatement. In this case, a Standard Form 86 must be completed. The five-year reinvestigation period is based on the date of the prior investigation, not on the date the DOE clearance is granted.

If no prior investigation or clearance can be verified, reciprocity does not apply and the applicant is processed for a new security clearance.

8. Interim Security Clearances

An Interim Security Clearance is used only for particularly sensitive positions. The TJSO must make a memorandum request to ORO, specifying the reason for the request and certifying the following:

- Serious delay or interference to an operation or project essential to a DOE program may occur, unless the person for whom the request is, is granted access to RD prior to completion of the authorization procedures.
- The services of a qualified person previously cleared or authorized access by DOE cannot be obtained.

The applicant must complete all the steps required for a security clearance as noted above; however, the ORO may grant an interim security clearance based upon a review of information available to them while awaiting a full investigative report from OPM.

NOTE: Interim security clearances may be extended or transferred for another purpose within the DOE complex only.

All individuals who are issued interim security clearances must be notified in writing that their continued security clearance is conditioned upon a favorable completion of the pending investigation, and may be canceled at any point where information of a security concern arises. Cancellations cannot be appealed and adjudication of the individual's eligibility for a security clearance will continue upon receipt of a completed investigation.

If DOE cancels an individual's interim security clearance, the FSO must ensure that the individual is precluded from access to classified information and SNM.

9. Temporary Security Clearance Upgrades

Temporary Security Clearance Upgrades may be available for current security clearance holders and requested for classified information or SNM one level higher that the individual's current security clearance (L to Q, Top Secret, Secret to Q or Top Secret, and any Confidential to L or

Secret). The upgrades are limited to specific, identifiable information, the nature of which must be stated on the request for access. They may only be used to meet operational or contractual requirements not expected to be a recurring nature, and may only last until the requirements have been fulfilled or until 180 calendar days, whichever is shorter. If information of a security concern arises that warrants the suspension/revocation of the permanent security clearance, the temporary security clearance will be canceled and action taken under 10 CFR 710 regarding the permanent clearance. Interim Security clearances may not be used as the basis for an upgrade and upgrades are not subject to reciprocity.

To request a Temporary Security Clearance Upgrade, the FSO shall prepare a DOE F 473.3, Clearance Access Request with justification including: the expected duration, a detailed description of the information to be accessed and the pressing situation prompting the request must be submitted to ORO. The upgrade request will be granted as long as the ORO is satisfied the following exigent circumstances exist, mission needs would not be adversely impacted by the processing of the higher security clearance, possession of information indicating that access at the higher level would not jeopardize Departmental interests or national security, and the request is not an attempt to circumvent normal processing requirements. The request will be denied and returned with an explanation for the decision should any of the above circumstances not be met. No due process or other procedural rights exist with regard to temporary security clearance upgrades.

Subsequent requests for temporary security clearance upgrades may be considered by ORO, in accordance with the procedures stated above. In addition, the package must include documentation necessary to process the individual for the required security clearance. Once the temporary clearance has been granted, the individual will be processed for the higher security clearance.

When an upgrade is issued, the individual will be under the general supervision of a fully cleared individual. The individual charged with supervising will be responsible for the general custody of the information provided.

10. Administrative Review Processing

ORO initiates an administrative review (AR), outlined in 10 CFR 710, when an individual's eligibility for security clearance has been suspended or cannot be granted because of unresolved security concerns. It gives the individual the opportunity to submit written information and/or to appear before a DOE hearing officer. ORO sends individuals processed under 10 CFR 710 explicit written information and instructions, including a point of contact to obtain further information.

When an individual's security clearance is denied or revoked following an AR, the individual is prohibited from requesting reconsideration of eligibility for a security clearance for a period of one (1) year from the date of their denial or revocation. After that time has elapsed, the individual may request reconsideration of eligibility from the director of the Office of Departmental Personnel Security, according to 10 CFR 710, only when the following circumstances exist:

- A bona fide offer of employment exists requiring access to RD, NSI, or SNM.
- Either (1) material and relevant new evidence exists, or (2) convincing evidence of rehabilitation or reformation exists.

The request for reconsideration must be submitted in writing to DOE and be accompanied by an affidavit detailing the new evidence or evidence of rehabilitation or reformation. The individual will be notified in writing if their reconsideration request has been approved. ORO will also be notified in writing of the approval. The individual will need to provide a copy of their reconsideration approval letter as proof before a new clearance request can be submitted to ORO.

11. Protection of Personnel Security Information

Because security clearance forms contain personally identifiable information, the forms must be protected according to the Privacy Act of 1974. Completed security forms will only be reviewed by designated employees trained in the procedures to check for adequacy and completeness before their submission to DOE. Employees with access to completed security forms for pre-employment- or pre-processing-check information and any other security clearance-related material must be informed of their responsibility to protect the information from unauthorized disclosure. All applicants for security clearances will have the opportunity to complete forms and submit documentation in private. Assistance in completing the forms will be provided by the FSO. Applicants are advised of Security's obligation to protect completed security forms and related materials on the Security Clearance Applicant/JSA Security Obligations form (Attachment 2) they are given during the clearance process.

Personnel security information relating to JSA clearance holders, including a Temporary Security Clearance Upgrade, is maintained by the FSO. Personal history statements are maintained by individuals who hold clearances. These protection measures include the following:

1. Storing Privacy Information – PII is stored in a locked drawer within a uniquely keyed office space, and may be discussed only with authorized persons in connection with the processing or adjudication of a security clearance, federal employment suitability determination, security inquiry, or criminal investigation. All correspondence to and from DOE that reflect security clearance matters must be maintained including the request for a security clearance, notification that security clearance action was effected, and security clearance termination and administrative withdrawal action.

2. Transmitting Privacy Information – The preferred method of transmitting PII is in person or telephonically directly to JSA or TJSO personnel. PII transmitted via email must be encrypted; PII transmitted by intra-office mail must be contained in an opaque envelope and marked with the caveat "To be opened by addressee only." Applicants can use regular mail to submit their personal information, but are encouraged to use express mail or Federal Express to better protect their information.

3. Destroying Privacy Information – Destruction of personal information records, when required, is accomplished in accordance with the manner prescribed for the destruction of OUO material. JSA utilizes a document destruction service to dispose of all sensitive and OUO materials.

4. Records Retention – Records must be maintained while an individual holds a security clearance and for a period of two (2) years after the date the clearance is terminated, at which time they may be destroyed.

12. Circumstances Affecting Security Clearance Change

When circumstances affecting an individual's security clearance change, the FSO and/or TJSO must notify ORO by completing and submitting a new DOE F 473.3, Clearance Access Request. Circumstances that require submittal of a new DOE F 473.3 include the following:

1. The Individual Accepted a Job in a Different DOE Element – The losing element must terminate the individual's security clearance because they are no longer performing duties requiring such a clearance. Upon JSA's request the TJSO will out-process the individual; have the individual complete a DOE F 5631.29, Security Termination Statement; and handwrite, "This individual is transferring to (Name of Element)" on the DOE F 5631.29. The TJSO must deliver that to ORO.

2. An Individual Had a Clearance that Was Terminated and Now Needs to be Reinstated – A clearance may be reinstated if the individual has remained under contract to DOE since the prior security clearance was terminated; the individual certifies on the SF 86 there has been no change in adjudicating relevant information. Generally, ORO will reinstate the clearance as long as there is no new or unresolved derogatory information. If the background investigation is still current (but not more than five years). Upon JSA's request for reinstatement, the TJSO must complete and submit to ORO a new DOE F 473.3, and provide a favorable drug test result.

3. An Individual Has an L, S, or C Clearance but Requires a Q or TS Clearance – The presumption is that the individual now has a need for access up to TS/RD or TS/NSI. Upon JSA's request, the TJSO must submit a DOE F 473.3 with a request for "Upgrade" in the justification block.

4. An Individual Has a Q or TS Clearance but Requires an L, S, or C Clearance – The individual no longer requires access up to TS/RD or NSI, but requires access up to C/RD or S/NSI. Upon JSA's request, the TJSO must submit a DOE F 473.3 with a request for "Downgrade" in the justification block.

5. An Individual Has a Clearance but No Longer Requires Access to Classified Information but Requires Regular Access to a HQ Facility – Upon JSA notification, the TJSO must submit a DOE F 473.3 with a request for "Downgrade to BAO" in the justification block. In addition, the TJSO has the individual complete the DOE F 5631.29, Security Termination Statement.

6. An Individual with a Security Clearance Needs to Support an Additional HQ Element – Upon JSA notification the applicant must submit a DOE F 473.3 with a request for "Extension" in the justification block. The extension allows ORO to identify all the headquarters elements that may have an interest in maintaining the individual's security clearance. Unless the individual will be working for more than one contractor, a security clearance extension is unnecessary if the individual is taking on additional duties within their sponsoring element.

7. TJSO Will No Longer Sponsor a Security Clearance – TJSO decides that the individual is leaving TJNAF. The TJSO must notify the individual of the decision and terminate their security clearance by completing a DOE F 5631.29 and providing it to ORO.

8. An Individual No Longer Requires a Security Clearance after Having Requested One – The FSO of an individual who is being processed for a security clearance but no longer needs it must submit an DOE F 473.3 with a request for "Cancellation" in the justification block.

9. Security Clearance Pending Reemployment/Reassignment – In the event a JSA employee with a security clearance is terminating employment but will be reemployed or reassigned by JSA within the next 60 calendar days to a position that will require a clearance, the FSO must prepare and submit a DOE F 473.3 to ORO requesting the individual to retain a security clearance.

13. Reportable Information and Reporting Requirements

The FSO facilitates all reporting requirements related to clearance holders at TJNAF. All individuals holding a security clearance and staff members assisting with the personnel security function have a specific obligation to report personnel security-related matters as they occur, whether related to themselves or to other individuals applying for or holding a DOE security clearance.

All notifications under this paragraph must be made within two (2) working days followed by a written confirmation within the next ten (10) working days unless otherwise noted.

JSA management has an obligation to report any condition affecting the status of an applicant's or employee's security clearance, including the following conditions:

JSA Management	Security Clearance Holder/FSO	Other Reporting with Guidance
Death of employee or applicant.	An immediate family member, to include a parent(s), brother(s), sister(s), spouse, or offspring assuming residence in a sensitive country. See the Sensitive Countries List, which is OUO, available from the FSO.	**Reporting 90 Day Absences:** Personnel granted an access authorization must report his/her marriage or cohabitation to the FSO. DOE F 5631.34, Data Report Spouse/Cohabitant, must be used to make the report to ORO and submitted within 45 days of the
Applicant declines an offer employment or fails to report to work.		
Termination	Any employment or association or	

JSA Management	Security Clearance Holder/FSO	Other Reporting with Guidance
Change in need to access classified information or access is restricted or withdrawn without DOE direction.	change in employment or association with a foreign or foreign-owned interest or representative, or non-U.S. citizen or other individual who is both a U.S. citizen and a citizen of a foreign country.	marriage or cohabitation. A National Agency Check (without fingerprints) is conducted on the spouse or cohabitant if not a U.S. citizen.
When made aware of any other information of a personnel security interest, as delineated in Attachment 4 of DOE O 472.2, CRD, concerning an applicant or employee.	Change in citizenship.	**Reporting Marriage and Cohabitation:** Personnel granted an access authorization must report his/her marriage or cohabitation to the FSO. DOE F 5631.34, Data Report on Spouse/Cohabitant, must be used to make the report to ORO and submitted within 45 days of the marriage or cohabitation. A National Agency Check (without fingerprints) is conducted on the spouse or cohabitant if not a U.S. citizen.
	Any arrests, criminal charges (including charges that are dismissed), citations, tickets, summons or detentions by federal, state, or other law enforcement authorities for violations of law within or outside of the U.S. Traffic violations for which a fine of up to $300 was imposed need not be reported, unless the violation was alcohol or drug-related.	
	Being hospitalized or entering an institution for the treatment of alcohol abuse, drug use, or mental or emotional condition, or otherwise being treated for such a condition.	
	Any use of an illegal drug, or the use of illegal drug in a manner that deviates from approved medical direction.	**Reporting Name Changes:** When a DOE-cleared individual has a name change, he/she must notify the FSO who will notify ORO, in writing, to ensure that the appropriate change is made to the security clearance record. ORO coordinates with the individual's servicing badge office and TJSO to obtain a corrected security badge.
	Personal or business-related filing for bankruptcy.	
	Garnishment of wages.	
	Legal action to effect a name change	

Table 4 – Reporting Change in Status

14. Reporting Unofficial Foreign Travel

Clearance holders must report all unofficial foreign travel plans to the FSO within 45 days before travel and must include the following information:

- Complete itinerary;
- Dates of travel;
- Mode(s) of transport, including identity of carriers;
- Passport data;
- Emergency point of contact;
- Names and association of foreign national traveling companions, and
- Planned interactions with foreign governments, companies or citizens during travel and reasons for contact (routine travel/tourism-related contacts excepted).

Non-Sensitive Countries

Reporting travel to a non-sensitive country does not require approval but the clearance holder is required to submit the Unofficial Foreign Travel Reporting Form (Attachment 4) as described above to the FSO and IN within 45 days before departure.

Sensitive Countries

Requests for travel to sensitive countries must be approved in writing by the clearance holder's supervisor or management chain. The request must be submitted no later than 90 days and no sooner than 180 days before departure. Management must request and consider applicable threat information from IN before making the decision to approve or deny the travel request. Clearance holders who are approved for travel to a sensitive country will receive appropriate briefings/debriefings from IN. The FSO will coordinate with IN for all such reporting and approval.

Decisions to disapprove travel to DOE sensitive countries can occur when it is determined that such travel presents an unacceptable risk to the Department, the physical safety and security of the clearance holder or to the security of classified matter. The grounds for any disapproval must be documented and, consistent with other laws, regulation and policy, shared with the clearance holder.

Clearance holders who are requesting travel to a sensitive country may appeal the disapproval decision to the TJSO ODFSA. The decision of the TJSO ODFSA is final. This may be delegated in writing to a senior Federal official.

Every effort will made to issue a decision to approve or disapprove travel in an expeditious manner. If, within 30 days of intention to travel to a sensitive country, a clearance holder has not received a decision and decides to travel anyway, this delay may be taken into consideration as a mitigating factor when assessing the traveler's failure to follow policy and whether this failure will impact their continued access and/or national security eligibility. Clearance holders assume all responsibility for any financial commitments made toward travel that is disapproved.

Deviations from approved sensitive country travel itineraries must be reported immediately upon return, but in no event greater than three working days upon returning to work.

Unplanned border crossings to Canada or Mexico must be reported within five business days of the occurrence.

When the need for emergency foreign travel precludes full compliance with the above requirements, verbal notification at a minimum shall be provided along with information concerning the nature of the emergency to the clearance holder's supervisor and the FSO. Full reporting shall be accomplished within five business days of return.

Upon return, the following information must be reported by the traveler to IN through the FSO, which will ensure it is communicated to ORO when a security concern is identified including the following:

- Unplanned interactions with foreign governments, companies or citizens, the reasons therefore (except routine travel/tourism-related contacts).
- Unusual or suspicious occurrences during travel, including those of a possible security or counterintelligence significance.

- Any foreign legal or customs incidents.

15. Contacts with Foreign Intelligence

Clearance holders must report all unofficial contacts with any known or suspected foreign intelligence entity to IN through the FSO. Reporting must occur immediately upon the clearance holder's cognizance of the situation, and in no event later than three working days upon returning to work. If this occurs while outside the U.S., reporting must occur immediately upon return to the traveler's normal duty station, and in no event more than three working days upon returning to work.

16. Elicitation

Attempted elicitation (to include by media sources), exploitation, blackmail, coercion or enticement to obtain classified matter or other information or material specifically prohibited by law from disclosure, regardless of means, must be reported by clearance holders to IN through the FSO immediately, and in no event later than three working days upon returning to work. Reporting is required regardless of whether the attempt results in a disclosure. If this occurs while outside the U.S., reporting must occur immediately upon return to the traveler's normal duty station, and in no event more than three working days upon returning to work.

17. Continuing Association with Foreign Nationals

Clearance holders must report to the FSO any unofficial continuing association with known foreign nationals that involves bonds of affection, personal obligation or intimate contact (Note: cohabitation with any foreign national, regardless of the nature of the relationship, must be reported).
This requirement is based on the nature of the relationship, regardless of how or where the contact was made or how the relationship is maintained (i.e. in person, telephonic, mail, internet, etc.).

After initial reporting, updates must be provided if and when there is a significant change in the nature of the contact.

"Continuing" contact is any contact which recurs, or which might reasonably be expected to recur, but does not include casual contact not based upon affection, obligation or intimacy.

Clearance holders must report to the FSO immediately after it becomes apparent that contact is continuing, and in no event later than three working days upon returning to work.

18. Foreign Activities

The following foreign activities must be reported by Clearance holders to the appropriate ORO immediately, but in no event later than three working days upon returning to work:

- Direct involvement in a foreign business

- Opening of a foreign bank account
- Purchase of a foreign property (whether located in a foreign country or not);
- Application for or receipt of foreign citizenship
- Application for, possession, or use of a foreign passport or identity card for travel
- Voting in a foreign election
- Adoption of a non-U.S. citizen child

19. Briefings

The following safeguards and security briefings are required for all security clearance holders. They serve as the means to instruct clearance holders in their duties and responsibilities related to the access afforded to them and to reiterate those duties and responsibilities upon termination of access.

Comprehensive Safeguards and Security Awareness Briefing
Personnel with DOE security clearances must receive a Comprehensive Security Awareness briefing, an online training through JSA upon receipt of a security clearance and before they may access classified matter or SNM. Documentation of the comprehensive briefing will be maintained in the JSA training system.

Refresher Safeguards and Security Awareness Briefing
Personnel with DOE security clearances must receive annual refresher briefings through the JSA training Office. Documentation of the refresher briefing will be maintained in the JSA training system.

Foreign Travel Briefing
Travel briefings required for JSA personnel holding DOE clearances are performed with prior arrangement with the DOE Office of Intelligence and Counterintelligence, Counterintelligence Directorate, Forrestal Field Office (IN). The FSO will coordinate pre-and post-trip travel briefings as required with the Forrestal Field Office.

Termination Briefing
Termination briefings are coordinated with the FSO or TJSO. The briefing must be documented by completing the Security Termination Statement Form (DOE F 5631.29), within two working days and communicated to ORO. In cases where it is not possible to obtain the individual's signature, the completed but unsigned form must still be submitted with an explanation surrounding the withdrawal and absence of signature.

20. Reinvestigations

Once a security clearance is granted, the individual must undergo a background reinvestigation every five years. Each fiscal year, ORO runs a report from the Central Personnel Clearance Index (CPCI) identifying all the Federal and contractor employees and consultants with security clearances in each HQ element due for reinvestigation. The report is sent to the TJSO as an

attachment to a memorandum requesting certain actions, which include:

- Ensuring that all personnel on the "due for reinvestigation" list still require security clearance.
- Ensuring that the clearance level for each person on the list is consistent with the person's actual access to classified information.
- Processing the required documents for reinvestigation.

The memorandum transmitting the list to the TJSO contains specific instructions. The TJSO will contact the FSO who will review reinvestigation list to ensure the person is still employed and still requires his/her security clearance.

If the person is no longer employed, or no longer needs a security clearance, his/her security clearance must be terminated. See aforementioned sections for details.

- The Individual Is No Longer at DOE
- The Individual Has Transferred to Another HQ Element
- The Individual Is Still Supporting the Element but No Longer Requires a Security Clearance

When the individual has a Q or TS security clearance and needs an L, S, or C clearance, or vice versa, the FSO must submit the documentation required to "Upgrade" or "Downgrade" the clearance in accordance with the instructions above.

When the individual needs to retain his/her current security clearance, the employee must complete a DOE F 5631.18, *Security Acknowledgement,* and submit it to the FSO.

The FSO processes a new DOE F 473.3, *Clearance Access Request*, marked as a "Reinvestigation," with the DOE F 5631.18 as an attachment, and submits both documents to ORO. The FSO ensures that the justification is complete and adequately explains the continued need for clearance. When the documents are approved, ORO advises the TJSO by e-mail to initiate the employee in e-QIP. See Section above for information on what actions the employee must take to complete e-QIP processing. The remainder of the process is described in section above, except that a new security badge is not issued to the employee.

When the individual fails to submit the documentation required for their reinvestigation or does not complete the e-QIP process within the prescribed timeframe, the individual is advised that such failure will result in rescinding or terminating their security clearance.

21. Clearance Verification

In addition to the list of reinvestigations, upon request, ORO runs a CPCI report identifying all TJNAF Federal and contractor employees and consultants, with active or pending security

clearances. The report is sent to the TJSO, and forwarded to the FSO as an attachment to a memorandum requesting that certain actions be taken. When possible, the packages are scanned and transmitted via encrypted e-mail. These actions include:
Ensuring that all the personnel on the list still require their security clearance.

Ensuring that the clearance level for each person on the list is consistent with the person's actual access to classified information.

Ensuring the office symbol for each employee is correct.
The memorandum transmitting the list to the TJSO contains specific instructions. The FSO reviews the verification list to confirm the person still requires the security clearance and remains assigned to the office shown.

If the person is no longer employed, has left the element, or no longer requires a security clearance, his/her security clearance must be terminated. The actions required for each scenario are detailed under Reinvestigations, above.

If the individual has a Q or TS security clearance and needs an L, S or C clearance, or vice versa, the FSO and TJSO will submit the documentation required to "Upgrade" or "Downgrade" the clearance in accordance with the instructions contained above.

When the individual has a different office symbol, the name of the employee must be highlighted on the verification list and their office symbol struck through with a line. The new office symbol must be handwritten beside the strikethrough.

Upon completion of the review, the entire list must be returned to ORO in accordance with the instructions contained on the original transmittal memorandum. This informs ORO that verification is complete and enables that office to update CPCI with the latest available information.

ATTACHMENT 1

Sample Letter
Reporting Results of Contractor Drug Testing

Date

Director, Office of Headquarters Personnel Security Operations
Office of Headquarters Security Operations
Office of Environment, Health, Safety and Security
U.S. Department of Energy
1000 Independence Avenue,
SW Washington, DC 20585

Dear Sir/Madam:

This letter is to inform you that (name of person) is an employee of this company and is applying for a Department of Energy security clearance. He/she has successfully completed drug testing requirements described in Title 10, Code of Federal Regulations (CFR), Part 707, and Title 48, CFR, Part 952.204-2.

(Name of person) was tested for the use of illegal substances. A copy of the laboratory report with favorable test results is enclosed with this letter.

If you have any questions concerning these matters, please call me at (757) 269-7548.

Sincerely,

Name
Facility Security Officer (or other official) Name of company

Enclosure (drug testing laboratory report)

ATTACHMENT 2

Jefferson Science Associates

Thomas Jefferson National Accelerator Facility

Security Clearance Applicant/JSA Security Obligations

I, _____, understand the following obligations are placed on me while completing all forms and documents that will be used in the adjudication of my Security Clearance Request, during the course of all personnel security investigations and at any stage of the security clearance process. Failure or refusal to cooperate with any of these activities may prevent DOE from granting or continuing a security clearance.

1. Provide assistance to DOE and Federal investigative agencies for conducting initial investigations.
2. Provide evidence of U.S. citizenship.
3. Provide full, frank and truthful answers to relevant and material questions.
4. Furnish or authorize others to furnish if necessary, information that DOE deems necessary to the security clearance eligibility process, when requested.
5. Report any situations listed on the Reporting Responsibilities.
6. Provide a completed DOE F 5631.34, Data Report on Spouse/Cohabitant, to the Security Officer within 45 calendar days of marriage or cohabitation.

In addition, I understand Security has the following obligations for the protection of personnel security information:

1. Completed security forms and all related material will only be reviewed by designated JSA employees for adequacy and completeness before being submitted to DOE, and that such information will not be used for any other purpose.
2. Security will maintain the following forms: DOE F 473.3, Clearance Access Request, DOE F 5631.18, Security Acknowledgement, Letter of Justification, Negative results from drug test, SF312. Per the Personnel Security Program Plan, all documents will be stored in a locked drawer within a uniquely keyed office space, and may only be discussed with authorized persons in connection with the processing or adjudication of a security clearance.
3. To obtain access to your personnel security folder, see the Facility Security Officer.
4. It is recommended that you keep copies of your completed security forms for personal records.

_____	_____	_____
Printed Name	Signature	Date

ATTACHMENT 3

DOE F 473.3
07/2019
(Replaces HQ F 5631.2)
All Other Editions Are Obsolete

U.S. Department of Energy Clearance Access Request

(Form becomes Official Use Only when filled in)

OMB Control No. 1910-1800

Submitting SON | DOE Number (if known)

CPSO | Primary Program Office Code(s) (i.e., EM, FE, IF, OE, SC, etc.) (If known)

Subject Information - All items in this section are mandatory

Employee Type | Employee email | Employee Phone

Name (Last, First, Middle, Suffix) | SSN | Date of Birth

Place of Birth (City, County, State (or Country if not U.S.))

Citizenship | Dual Citizenship Country (if applicable)

Dual Citizen? | Additional Dual Citizenship Country (if applicable)

Job Title | Work Location

If individual is a Contractor Incumbent, Contractor Applicant, or Contractor Consultant, complete applicable items

Prime Contract Company | If Subcontractor, Company Name

Prime Contract Number | Sub Contractor Contract Number (if applicable)

Prime Contract Expiration Date | Sub-Contract Expiration Date (if applicable)

Employing Company Facility Security Officer POC & Phone | Employer Code | Facility Code | Is Subject a KMP?

Clearance, Access, and Justification - All items in this section are mandatory

Action Requested | Current Clearance Level of Subejct | Current Clearance Required

Will Subject be submitted for a SAP?

Justification: Provide detailed information (***without revealing classified data***) as to why the Subject requires access. This description must include a full explanation of the information to be accessed, frequency of access, and for what programs/projects the information is needed.

To be filled out by the Cognizant Personnel Security Office receiving the completed Clearance Access Request Form

May be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). Department of Energy review required before public release.

Exemption number & category | Name/Org | Date

Guidance (if applicable)

Documents: (Check all that apply and forward to DOE Personnel Security.) (Request will not be processed until all checked Documents are received) Per DOE O 472.2, Attachment 2, paragraph 2.a. - 2.f: All initial security clearance requests (to include requests for reinstatements and reapprovals) must include the justification, as set forth above, and all boldfaced items (except in cases where reciprocity applies, as indicated by an '*'):

- ☐ **Proof of Negative Drug Screen Results:** Results of drug test within 60 calendar days of the individual's e-QIP signature or, for cases being considered under reciprocity, within 60 calendar days of the date of the security clearance request (not required for state or local governments)
- ☐ ***e-QIP:** A complete e-QIP submission which indicates no illegal use of controlled substances for at least 12 months preceding the individual's signature.
- ☐ ***Fingerprints:** Fingerprints taken electronically via an approved capture method (e.g., at a GSA-provided HSPD-12 enrollment center) (not required if a previous investigation included a classifiable fingerprint search by FBI).
- ☐ ***Resume or OF 612, Optional Application for Federal Employment:** Federal Applicants and Employees Only.
- ☐ **DOE F 5631.18**, Security Acknowledgment
- ☐ ***Fair Credit Reporting Disclosure and Authorization:** A completed fair credit reporting disclosure authorization, compliant with the Fair Credit Reporting Act, codified at 15 U.S.C. s1681 et seq. and approved for use by the Director (once obtained, this authorization may be used by DOE for conducting credit checks directly with consumer agencies as part of its personnel security program.
- ☐ Other (i.e., Birth Certificate, Certificate of Naturalization, Reinvestigation documentation, etc..)(Specify below)

Certifications (as applicable)

By signing below I hereby certify the individual listed in this request is required to possess a security clearance at the level indicated and that the job, duties, access areas, and classified information access listed are an accurate description of the individual's position.

Requesting Official/Supervisor Signature		Requesting Official/ Supervisor Name/Title/Phone	
Contractor Certifying Official Signature		Contractor Certifying Official Name/Title/Phone	
Federal Certifying Official Signature		Federal Certifying Official Name/Title/Phone	

Date Clearance Access Request forwarded to DOE Personnel Security

DOE Personnel Security Signature		DOE Personnel Security Official Title/Phone	

OMB BURDEN DISCLOSURE STATEMENT

Public reporting burden for this collection of information is estimated to average 3 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Office of Management, MA-90, GTN, Paperwork Reduction Project (1910-1800), U.S. Department of Energy, 1000 Independence Ave., SW, Washington, DC 20585-1290; and to the Office of Management and Budget (OMB), Paperwork Reduction Project (1910-1800), Washington, DC 20503.

PRIVACY ACT STATEMENT

The Department of Energy (DOE) will use the information collected through this form to process requests for an individual to possess a security clearance and access authorization, including requests for reinstatements and reapprovals. 42 U.S.C. 7101 et seq., 50 U.S.C. 2401 et seq., 10 C.F.R. Part 710, and Executive Orders 13764, 10865, and 13526 authorizes DOE collection of this information. DOE may disclose this information to ensure routine information sharing relevant to the processing of an access authority or clearance, including to DOE contractors in performance of their contracts, and their officers and employees who have a need for the record in the performance of their duties; competent medical authorities to determine whether an individual has an illness or mental condition of a nature which causes, or may cause, a significant defect in judgment or reliability, or is alcohol dependent or suffering from alcohol abuse; or other federal, state, or local agencies for official business purposes and validation of information related to the decision to grant access authority or a security clearance. Additionally, DOE may disclose this information to members of Congress, making requests on behalf of a constituent; and to local, state, or federal agencies for the purposes of law enforcement. If the individual elects not to provide the requested information on this form, it could result in a delay in (or denial of) processing this request (or any future request for reinstatement) of the individual's DOE access authorization/security clearance. An individual's DOE access authorization/security clearance can be terminated regardless of whether this form is completed. An individual's name and Social Security Number are used as identifying factors to establish and maintain records of DOE access authorization actions in the DOE System of Records, DOE-43, "Personnel Security Files." This form will be completed and maintained in the individual's DOE Personnel Security File.

Instructions

CPSO: Use the drop-down list to select the appropriate Cognizant Personnel Security Office that is responsible for security clearance processing.

Submitting SON: Enter the Submitting Office Number identifier of the office submitting the request.

DOE Number: Enter Subject's DOE Number, if known or applicable.

Primary Program Code: Enter the code for the primary program to which Subject will be assigned, if known.

Subject Information - All items in this section are mandatory:

Employee Type: Use the drop-down list to choose the appropriate employee type for individual.

Employee email: Enter the employee's primary email address.

Employee Phone: Enter employee's primary phone.

Name: Enter individual's full legal name, including full middle name.

SSN: Enter the individual's full Social Security Number

Date of Birth: Use the calendar to select the Subject's date of birth, or manually enter in DD/MM/YYYY format.

Place of Birth: Enter city, county, state (or country if not U.S.) where Subject was born.

Citizenship: Choose appropriate country of individual's citizenship.

Dual Citizen: Use drop-down to select Yes or No. If Yes, then use drop-down lists to complete **Dual Citizenship Country** fields as applicable.

Job Title: Enter the Subject's job title.

Work Location: Enter location where Subject will work.

If individual is a Contractor Incumbent, Contractor Applicant, or Contractor Consultant, complete applicable items

Prime Contract Company: Enter the prime contractor company's name.

If Subcontractor, Company Name: Complete if individual works for one of the sub-contractors.

Employing Company Facility Security Office POC & Phone: Enter the Facility Security Office information for the company which employs the Subject.

Facility Code: Enter the employing company's Facility Code.

Employer Code: Enter employing company's Employer Code.

Contract Number: Enter the contract number for the Prime Contract.

Sub Contractor Contract Number (if applicable: If individual works a subcontractor, enter the Sub-contract number.

Contract Expiration Date: Use the Calendar to select the date the Prime contract expires, or manually enter in DD/MM/YYYY format..

Sub-Contract Expiration Date (if applicable): If applicable, enter the expiration date of the sub-contract, or manually enter date in DD/MM/YYYY format.

Is Subject a KMP?: Use drop-down list to select Yes or No to indicate if Subject is a Key Management Person for the company.

Clearance, Access, and Justification - All items in this section are mandatory

Action Requested: Use drop-down list to select appropriate action being requested.

Current Clearance Level of Subject: Use the drop-down list to select the Subject's **current** clearance level. If the Subject does not currently have a clearance, select Uncleared.

Clearance Level Required: Use the drop-down list to select the clearance level required for Subject to preform their duties.

Will Subject be submitted for a SAP: Use the drop-down list to select Yes or No.

Justification: Per DOE Order 472.2, Attachment 2, paragraph 1.i.: "A detailed description (without revealing classified information) as to why the individual requires access. The description must include a full explanation of the information to be accessed, how often the access is needed, and for what programs/projects the information is needed." Insufficient justification will be cause for rejection of request.

Exemption Section
To be filled out by the Cognizant Personnel Security Office receiving the completed Clearance Access Request Form

Documents Required

Check all that apply. Request will not be processed until all checked enclosures are received. Per DOE O 472.2, Attachment 2, paragraph 2.a. - 2.f: All initial security clearance requests (to include requests for reinstatements and reapprovals) must include the justification, as set forth above, and all boldfaced items (except in cases where reciprocity applies, as indicated by an '*').

Certifications (as applicable)
NOTE: If signers have a PIV, then electronic signature is requested.

Requesting Official: Person completing the request. This can be the person responsible for submitting the contractor requests, or if Subject is a Federal Applicant/Incumbent, then this can be the Supervisor, HC representative, office director, etc.

Contractor Certifying Official: The Certifying Official is responsible for certifying the clearance is required per all applicable laws, rules and regulations.

Federal Certifying Official: This can be the COR, COTR, or their designee for contractor positions. If local processes require Site Manager or other federal certifying official to approve the clearance access request, this is where this person signs. HSO (DOE HQ ONLY) signs here if the request will be processed by DOE Headquarters Personnel Security.

Date Clearance Access Request forwarded to DOE Personnel Security: Use calendar to select the date the clearance access request is sent to the appropriate CPSO, , or manually enter date in DD/MM/YYYY format.

T JSA Jefferson Science Associates)

Thomas Jefferson National Accelerator Facility

CLEARANCE HOLDER
UNOFFICIAL FOREIGN TRAVEL REPORTING FORM

PART 1 – PERSONAL INFORMATION

Last Name: _____ First Name: _____ MI _____ Suffix: _____

Passport No. _____ Visa No./Country: _____

Office Phone No. _____ Cell: _____

Personal Phone No.: _____ Cell: _____

PART II – EMERGENCY POINT OF CONTACT

Please provide the requested information for a domestic point of contact not traveling with you.

Last Name: _____ First Name: _____ MI _____ Suffix: _____

Relationship:_____ Phone No.: _____ Cell No._____

Street: _____

City: _____ State: _____ Zip Code: _____

PART III – REASON FOR TRAVEL (Other than vacation)

_____

_____

PART II – ITINERARY OVERVIEW

Countries to be Visited	Major Cities	Dates: From/To
1.		
2.		
3.		

PART III – TRAVEL INFORMATION

Please provide specific information for each destination of travel using additional paper, if needed. A new Travel Information page must be completed for each destination to be visited. Alternatively, attach itinerary and email all documents to fso@jlab.org. ☐ **See Attached Itinerary**

Country Details:

Country: _____ City: _____

Date From: _____ Date To: _____

1. **Mode of Transportation (Check all that apply or attach itinerary):**

☐ Plane Carrier: _____ Flight No(s).:_____

☐ Cruise Cruise Line: _____ Cruise No.: _____

Ship Name: _____ Country of Registry: _____

☐ Train Carrier: _____ ☐ Boat: _____

☐ Rental Car Company:_____ ☐ Other:_____

2. **Accommodations/Lodging:**

Name/Place: _____ Room No. (if known)_____

Phone No.: _____Address: _____

Are you traveling with a foreign national? ☐ Yes ☐ No If "Yes," list below:

Name of Foreign National	Nature of Association (Business, relative, friend, etc.)	Full Address	Citizenship

Are you planning to make contact with foreign governments, companies, or citizens upon your arrival at this location? ☐ Yes ☐ No If "Yes," list below:

Foreign Government and/or name of Company or Individual	Reason for Contact (Business, relative, friend, etc.)	Full Address	Citizenship

Are you traveling with any dependents? ☐ Yes ☐ No If "Yes", how many? _____

*This information is requested to account for you and your dependents in the event of an emergency and is optional.

PART V – ADDITIONAL COMMENTS

Please email completed form to fso@jlab.org.

_____ _____

Traveler Signature Date