NASHVILLE DISTRICT (LRN) SECURITY CONTRACT REQUIREMENTS

(CATEGORY B-1) UP TO SIX (6) MONTHS
NASHVILLE DISTRICT (LRN) SECURITY CONTRACT REQUIREMENTS
U.S. CITIZEN CONTRACTOR - ACCESS REQUIRED TO LRN CRITICAL INFRASTRUCTURE,
GOVERNMENT INFORMATION SYSTEMS, OR GOVERNMENT FUNDS

Standard Limited Criminal Check: All Contractor and Subcontractor employees (hereinafter CSE) working under this contract or applicable task orders, regardless of type or length of contract will undergo a limited criminal check based on LEXIS/NEXIS (LN) conducted by the Nashville District Security Management Office (LRN-SM). The CSE submits legible documents or photocopies to the Contractor or the Contractor's designated representative (hereinafter, Contractor) who is responsible for submitting the required documents to the COR for a LN check, 10 calendar days prior to CSE access to the project:

1. **LRN U.S. Citizen Security Access Form** – **The form and guidance is available at**
https://www.lrd.usace.army.mil/Submit-ArticleCS/Programs/Article/3667149/contracting/

2. **Pre-Screen Candidates using E-Verify Program**: The Contractor must pre-screen candidates using the E-Verify program (http://www.uscis.gov/e-verify) website to meet the established employment eligibility requirements. The Vendor must ensure that the Candidate has two valid forms of Government issued identification prior to enrollment to ensure the correct information is entered into the E-verify system. An initial list of verified/eligible candidates must be provided to the COR no later than three (3) business days after the initial contract award and a minimum of five (5) business days for new candidates thereafter.

3. **Photocopy of Two (2) IDs Provided for e-Verify**: Acceptable documents are listed on the Form I-9. (This form can be found at the web address in #2 above.)

4. **Declaration for Federal Employment (OF-306):** The OF-306 must be typed/dated/signed. The **latest form must be used** and is available with detailed instructions from OPM at https://www.opm.gov/forms/optional-forms/. CSE shall answer completely and truthfully, as any false statement could result in termination of approval and ability to work.

5. **Fingerprints may also be required based on LN/JX results.** If so, the individual will not be authorized to work until fingerprint results are received and the Contractor has been notified by the COR. Fingerprint guidance can be found at **http://www.lrn.usace.army.mil/BusinessWithUs/Contracting/Contract Security Requirements**

U.S. Citizen Born Outside the United States – In addition to requirements above, documentation shall be submitted which verifies the CSE is a U.S. Citizen: U.S. Passport (unexpired or expired), Certificate of U.S. Citizenship (INS Form N-560 or N-561), Certificate of Naturalization (INS Form N-550 or N-570), Consular Report of Birth Abroad (Form FS-240), or Certificate of Report of Birth (DS-1350).

Approval/Disapproval: The COR will notify the Contractor when the CSE is permitted to access security sites.

Approval: If the results are favorable, the COR will notify the Contractor in writing that the CSE is approved to begin work. The COR and the Contractor shall ensure the CSE is off-site by the expiration of the six-month approval.

Disapproval: If a favorable determination could not be made, the COR will notify the Contractor that the CSE is not approved to work on the contract.

All approvals with restrictions, or disapprovals provided by LRN-SM shall be considered final with no appeal rights for the Contractor or CSE under review.

Record Keeping: The COR and the Contractor will be responsible for ensuring only approved CSEs are given access to the work site. An example of a CSE Contractor spreadsheet to assist you in tracking this is available through the COR. The Contractor and COR shall be responsible for protecting all sensitive personal information such as social security numbers, birth dates, etc. Anyone who handles PII should be trained annual at: https://www.cdse.edu/Training/eLearning/DS-IF101. For more information on PII safeguarding and reporting visit: https://www.dami.army.pentagon.mil/site/infosec/docs/Pub/Army%20PII%20User's%20guide.pdf.