3452.204-71 Contractor security vetting requirements.

As prescribed in 3404.470–1, insert the following clause:

Contractor Security Vetting Requirements (OCT 2023)

(a) The Contractor and its subcontractors shall comply with Department of Education personnel, cyber, privacy, and security policy requirements set forth in "Contractor Security Vetting Requirements" at *http://www.ed.gov/fund/contract/about/bsp.html*.

(b) Contractor employees who will have access to proprietary or sensitive Department information including "Controlled Unclassified Information" as defined in 32 CFR 2002.4(h), Department IT systems, Contractor systems operated with Department data or interfacing with Department systems, or Department facilities or space, or perform duties in a school or in a location where children are present, must undergo a personnel security screening and receive a favorable determination and are subject to reinvestigation as described in the "Contractor Vetting Security Requirements." Compliance with the "Contractor Vetting Security Requirements," as amended, is required.

(c) The type of security investigation required to commence work on a Department contract is dictated by the position designation determination assigned by the Department. All Department Contractor positions are designated commensurate with their position risk/sensitivity, in accordance with title 5 of the Code of Federal Regulations (5 CFR 731.106) and OPM's Position Designation Tool (PDT) located at: *https://pdt.nbis.mil/*. The position designation determines the risk level and the corresponding level of background investigations required.

(d) The Contractor shall comply with all Contractor position designations established by the Department.

(e) The following are the Contractor employee positions required under this contract and their designated risk levels:

High Risk (HR): (Specify HR positions or Insert "Not Applicable")

Moderate Risk (MR): (Specify MR positions or Insert "Not Applicable")

Low Risk (LR): Specify LR positions or Insert "Not Applicable")

(f) For performance-based contracts where the Department has not identified required labor categories for Contractor positions, the Department considers the risk sensitivity of the services to be performed and the access to Department facilities and systems that will be required during performance, to determine the uniform Contractor position risk level designation for all Contractor employees who will be providing services under the contract. The uniform Contractor position risk level designation applicable to this performance-based contract is: (Contracting Officer to complete with overall risk level; or insert "Not Applicable").

(g) Only U.S. citizens will be eligible for employment on contracts requiring a Low Risk/Public Trust, Moderate Risk/Public Trust, High Risk/Public Trust, or a National Security designation.

(h) An approved waiver, in accordance with the “Contractor Vetting Security Requirements,” is required for any exception to the requirements of paragraph (g) of this section.

(i) The Contractor shall—

(1) Comply with the Principal Office (PO) processing requirements for personnel security screening;

(2) Ensure that no Contractor employee is placed in a higher risk position than for which the employee is approved;

(3) Ensure Contractor employees submit required security forms for reinvestigation in accordance with the time frames set forth in the “Contractor Vetting Security Requirements”;

(4) Report to the COR any information (*e.g.,* personal conduct, criminal conduct, financial difficulties) that would raise a concern about the suitability of a Contractor employee or whether a Contractor employee's continued employment would promote the efficiency of the service or violate the public trust;

(5) Protect sensitive and Privacy Act-protected information, including “Controlled Unclassified Information” as defined in 32 CFR 2002.4(h), from unauthorized access, use, or misuse by its Contractor employees, prevent unauthorized access by others, and report any instances of unauthorized access, use, or misuse to the COR;

(6) Report to the COR any removal of a Contractor employee from a contract within one business day if removed for cause or within two business days if otherwise removed;

(7) Upon the occurrence of any of the events listed under paragraph (b) of the clause at FAR 52.204–9, Personal Identity Verification of Contractor Personnel, return a PIV ID to the COR within seven business days of the Contractor employee's departure; and

(8) Report to the COR any change to job activities that could result in a change in the Contractor employee's position or the need for increased security access.

(j) Failure to comply with any of the personnel security requirements in the “Contractor Security Vetting Requirements” at *http://www.ed.gov/fund/contract/about/bsp.html*, may result in a termination of the contract for default or cause.

(End of clause)

Parent topic: Subpart 3452.2—Text of Provisions and Clauses