



UNITED STATES DEPARTMENT OF EDUCATION
OFFICE OF FINANCE AND OPERATIONS

December 10, 2019

ACQUISITION ALERT 2020-01

TO: Heads of Contracting Activities
Office of Finance and Operations/Contracts and Acquisitions Management
Federal Student Aid/Federal Student Aid Acquisitions
Executive Officers

FROM: James M. Hairfield 
Acting Deputy Assistant Secretary for Acquisition Management

SUBJECT: Education Acquisition Regulation (EDAR) Class Deviation: Cyber and Personnel
Security Requirements for Contractors

1. **Purpose:** The purpose of this alert is to issue a class deviation to ensure active contracts, solicitations, and future contracts communicate ED's cybersecurity and personnel security screening requirements to contractors and prospective contractors.
2. **Deviated Language:** EDAR Part 3439 – Acquisition of Information Technology; EDAR Part 3452 Solicitation Provisions and Contract Clauses
3. **Applicability:** This deviation applies to all solicitations and contracts where contractor personnel will have access to proprietary or sensitive ED information, including “Controlled Unclassified Information” as defined in 32 CFR Part 2002, ED Information Technology (IT) systems, systems maintained on behalf of ED, ED facilities/space, and/or perform duties in a school or in a location where children are present.
4. **Background:** ED memorandum “Interim Personnel Security Requirements and Guidance to Support Access to Department Information, Information Systems, and Facilities” dated August 22, 2018, and OCIO: 3-112, “Cybersecurity Policy” dated April 12, 2019, including “Controlled Unclassified Information” as defined in 32 CFR Part 2002, set forth ED's Contractor Employee Personnel Screening and Cybersecurity policy. The provision at 3452.239-71 “Notice to offerors of Department security requirements” and the clause at 3452.239-72 “Department security requirements” do not comply with the stated ED policy. This class deviation provides a replacement provision and clause that accurately reflects the current ED policy. The associated prescription for use at 3439.702 is also revised to comply with ED's current policy.
5. **Effective Date:** Immediately
6. **Expiration Date:** Effective until incorporated into the EDAR or otherwise rescinded.

7. **Required Action:** Contracting officers shall include the provision, 3452.239-71 “Notice to offerors of Department security requirements (DEVIATION)”, and clause, 3452.239-72 “Department security requirements (DEVIATION)” in all new solicitations and contracts, as applicable. Within 90 days contracting officers shall modify existing contracts, to include 3452.239-72 “Department security requirements (DEVIATION)”, as applicable. See Attachment C, “Frequently Asked Questions,” for additional information.
8. **Attachments:**
 - A. Class Deviation signed by Chief Acquisition Officer, dated December 6, 2019
 - B. Deviated Language of EDAR 3439.702, 3452.239-71 and 3452.239-72
 - C. Frequently Asked Questions
9. **Additional Information:** Eileen McGlinn at eileen.mcglinn@ed.gov

Prescription for use (applies to, both, 3452.239-71 and 3452.239-72):

3439.702 Department security requirements (DEVIATION).

The contracting officer must include the solicitation provision in 3452.239-71 (DEVIATION) (Notice to offerors of Department security requirements) and the clause at 3452.239-72 (DEVIATION) (Department security requirements) when contractor employees will have access to proprietary or sensitive ED information including “Controlled Unclassified Information” as defined in 32 CFR Part 2002, ED Information Technology (IT) systems, systems maintained on behalf of ED, ED facilities/space, and/or perform duties in a school or in a location where children are present.

Deviated provision 3452.239-71:

3452.239-71 Notice to offerors of Department security requirements (DEVIATION)

As prescribed in 3439.702, include the following provision in solicitations when the offeror’s employees would have access to proprietary or sensitive ED information including “Controlled Unclassified Information” as defined in 32 CFR Part 2002, ED Information Technology (IT) systems, systems maintained on behalf of ED, ED facilities/space, and/or perform duties in a school or in a location where children are present:

Notice to offerors of Department security requirements (DEVIATION)

- (a) The successful contractor must comply with Department of Education personnel, cyber, and privacy security policy requirements as set forth in “Security Requirements for Contractors Doing Business with the Department of Education” at <http://www.ed.gov/fund/contract/about/bsp.html>.
- (b) Contractor employees who will have access to proprietary or sensitive ED information including “Controlled Unclassified Information” as defined in 32 CFR Part 2002, or ED IT systems, systems maintained on behalf of ED, ED facilities or space, and/or perform duties in a school or in a location where children are present, must undergo a personnel security screening and a favorable determination and are subject to reinvestigation as described in the “Contractor Vetting Security Requirements.” Compliance with these “Contractor Vetting Security Requirements,” is required.
- (c) The type of security investigation required to commence work on an ED contract is dictated by the position designation determination assigned by ED. All ED contractor positions are designated commensurate with their position risk/sensitivity, in accordance with Title 5 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 ED.

Attachment B

(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 ED has not identified required labor categories for contractor positions, ED considers the risk sensitivity of the services to be performed and the access to ED 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 Moderate Risk/Public Trust, High Risk/Public Trust, or a National Security designation.

(h) Permanent resident aliens may be eligible for employment on contracts requiring Low Risk/Public Trust access.

(i) An approved waiver, in accordance with "Contractor Vetting Security Requirements" is required for any exception to the requirements of paragraph (g) and (h) above.

(j) Performance of this contract will will not involve access to ED IT systems and/or systems maintained on behalf of ED. For contracts that require access to ED IT systems and/or systems maintained on behalf of ED, the Information Security Categorization applicable to each security objective has been determined to be:

Confidentiality: Low Moderate High *(Contracting Officer to complete)*

Integrity: Low Moderate High *(Contracting Officer to complete)*

Availability: Low Moderate High *(Contracting Officer to complete)*

Overall Risk Level: Low Moderate High *(Contracting Officer to complete)*

(k) Performance of this contract does involve does not involve Personally Identifiable information (PII). The PII Confidentiality Impact Level has been determined to be:

Not Applicable Low Moderate High.

(End of Provision)

Deviated clause 3452.239-72:

3452.239-72 Department security requirements. (DEVIATION)

As prescribed in 3439.702, include the following clause in contracts when the contractor's employees will have access to proprietary or sensitive ED information including "Controlled Unclassified Information" as defined in 32 CFR Part 2002, ED Information Technology (IT) systems, systems maintained on behalf of ED, ED facilities/space, and/or perform duties in a school or in a location where children are present:

Department Security Requirements (DEVIATION)

(a) The contractor and its subcontractors shall comply with Department of Education personnel, cyber, and privacy, security policy requirements as set forth in "Security Requirements for Contractors Doing Business with the Department of Education" at <http://www.ed.gov/fund/contract/about/bsp.html>.

(b) Contractor employees who will have access to proprietary or sensitive ED information including "Controlled Unclassified Information" as defined in 32 CFR Part 2002, or ED IT systems, systems maintained on behalf of ED, ED facilities or space, and/or perform duties in a school or in a location where children are present, must undergo a personnel security screening and a favorable determination and are subject to reinvestigation as described in the "Contractor Vetting Security Requirements." Compliance with these "Contractor Vetting Security Requirements," as amended, is required.

(c) The type of security investigation required to commence work on an ED contract is dictated by the position designation determination assigned by ED. All ED contractor positions are designated commensurate with their position risk/sensitivity, in accordance with Title 5 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 ED.

(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 ED has not identified required labor categories for contractor positions, ED considers the risk sensitivity of the services to be performed and the access to ED 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")

Attachment B

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

(h) Permanent resident aliens may be eligible for employment on contracts requiring Low Risk/Public Trust access.

(i) An approved waiver, in accordance with "Contractor Vetting Security Requirements" is required for any exception to the requirements of paragraphs (g) and (h) above.

(j) 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 he or she is approved,
- (3) Ensure contractor employees submit required security forms for reinvestigation in accordance with the timeframes set forth in the "Contractor Vetting Security Requirements,"
- (4) Report to the COR any information (i.e., personal conduct, criminal conduct, financial difficulties, etc.) that would raise a concern about the suitability of a contractor 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, including "Controlled Unclassified Information" as defined in 32 CFR Part 2002, 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 within two business days any removal of a contractor employee from a contract; or within one business day if removed for cause,
- (7) Return a PIV ID to the COR within seven business days of the contractor employee's departure,
- (8) Report to COR of any job activities that contractor employee has brought to their attention that they believe could result in a change in the contractor employee's position or the need for increased security access; and
- (9) Ensure that any ED information processed, stored, or transmitted by the contractor will not be used or redistributed except as specified in the contract.

(k) Performance of this contract will will not involve access to ED IT systems and/or systems maintained on behalf of ED. For contracts that require access to ED IT systems and/or systems maintained on behalf of ED, the Information Security Categorization applicable to each security objective has been determined to be:

Confidentiality: Low Moderate High (Contracting Officer to complete)

Integrity: Low Moderate High (Contracting Officer to complete)

Attachment B

Availability: Low Moderate High (Contracting Officer to complete)

Overall Risk Level: Low Moderate High (Contracting Officer to complete)

(l) Performance of this contract does involve does not involve Personally Identifiable information (PII) or "Controlled Unclassified Information" as defined in 32 CFR Part 2002. The Confidentiality Impact Level of such information has been determined to be:

Not Applicable Low Moderate High. _

(m) Failure to comply with any of the personnel, privacy, and cyber security requirements may result in a termination of the contract for default or cause.

(End of Clause)