Department of Education

personnel receive early dismissal instructions.

(b) In cases of contract performance at a Government facility when the facility is closed, the vendor may arrange for performance to continue during the closure at the contractor's site, if appropriate.

(End of clause)

3452.239–70 Internet protocol version 6 (IPv6).

As prescribed in 3439.701, insert the following clause in all solicitations and resulting contracts for hardware and software:

INTERNET PROTOCOL VERSION 6 (MAR 2011)

(a) Any system hardware, software, firmware, or networked component (voice, video, or data) developed, procured, or acquired in support or performance of this contract shall be capable of transmitting, receiving, processing, forwarding, and storing digital information across system boundaries utilizing system packets that are formatted in accordance with commercial standards of Internet protocol (IP) version 6 (IPv6) as set forth in Internet Engineering Task Force (IETF) Request for Comments (RFC) 2460 and associated IPv6-related IETF RFC standards. In addition, this system shall maintain interoperability with IPv4 systems and provide at least the same level of performance and reliability capabilities of IPv4 products.

(b) Specifically, any new IP product or system developed, acquired, or produced must—

(1) Interoperate with both IPv6 and IPv4 systems and products; and

(2) Have available contractor/vendor IPv6 technical support for development and implementation and fielded product management.

(c) Any exceptions to the use of IPv6 require the agency's CIO to give advance, written approval.

(End of clause)

3452.239–71 Notice to offerors of Department security requirements.

As prescribed in 3439.702, include the following provision in solicitations when the offeror's employees would have access to Department-controlled facilities or space, or when the work (wherever located) would involve the design, operation, repair, or maintenance of information systems and access to sensitive but unclassified information:

DEPARTMENT SECURITY REQUIREMENTS (MAR 2011)

(a) The offeror and any of its future subcontractors will have to comply with Department security policy requirements as set forth in the “Bidder's Security Package: Security Requirements for Contractors Doing Business with the Department of Education” at: http://www.ed.gov/fund/contract/about/bsp.html.

(b) All contractor employees must undergo personnel security screening if they will be employed for 30 days or more, in accordance with Departmental Directive OM:5–101, “Contractor Employee Personnel Security Screenings,” available at: http://www.ed.gov/fund/contract/about/acs/acsom5101.doc.

(c) The offeror shall indicate the following employee positions it anticipates to employ in performance of this contract and their proposed risk levels based on the guidance provided in Appendix I of Departmental Directive OM:5–101:

High Risk (HR): [Specify HR positions.]

Moderate Risk (MR): [Specify MR positions.]

Low Risk (LR): [Specify LR positions.]

(d) In the event the Department disagrees with a proposed risk level assignment, the issue shall be subject to negotiation. However, if no agreement is reached, the Department's risk level assignment shall be used. The type of screening and the timing of the screening will depend upon the nature of the contractor position, the type of data to be accessed, and the type of information technology (IT) system access required. Personnel security screenings will be commensurate with the risk and magnitude of harm the individual could cause.

(End of provision)

3452.239–72 Department security requirements.

As prescribed in 3439.702, include the following clause in contracts when the contractor's employees will have access to Department-controlled facilities or space, or when the work (wherever located) would involve the design, operation, repair, or maintenance of information systems and access to sensitive but unclassified information:

DEPARTMENT SECURITY REQUIREMENTS (MAR 2011)

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

High Risk (HR): [Specify HR positions.]
Moderate Risk (MR): [Specify MR positions.]
Low Risk (LR): [Specify LR positions.]

(c) All contractor employees must undergo personnel security screening if they will be employed for 30 days or more, in accordance with Departmental Directive OM:5–101, “Contractor Employee Personnel Security Screenings.” The type of screening and the timing of the screening will depend upon the nature of the contractor position, the type of data to be accessed, and the type of information technology (IT) system access required. Personnel security screenings will be commensurate with the risk and magnitude of harm the individual could cause.

(d) The contractor shall—

(1) Ensure that all non-U.S. citizen contractor employees are lawful permanent residents of the United States or have appropriate work authorization documents as required by the Department of Homeland Security, Bureau of Immigration and Appeals, to work in the United States.

(2) Ensure that no employees are assigned to high risk designated positions prior to a completed preliminary screening.

(3) Submit all required personnel security forms to the contracting officer’s representative (COR) within 24 hours of an assignment to a Department contract and ensure that the forms are complete.

(4) Ensure that no contractor employee is placed in a higher risk position than that for which he or she was previously approved, without the approval of the contracting officer or the COR, the Department personnel security officer, and the Department computer security officer.

(5) Ensure that all contractor employees occupying high-risk designated positions submit forms for reinvestigation every five years for the duration of the contract or if there is a break in service to a Department contract of 365 days or more.

(6) Report to the COR all instances of individuals seeking to obtain unauthorized access to any departmental IT system, or sensitive but unclassified and/or Privacy Act protected information.

(7) Report to the COR any information that raises an issue as to whether a contractor employee’s eligibility for continued employment or access to Department IT systems, or sensitive but unclassified and/or Privacy Act protected information, promotes the efficiency of the service or violates the public trust.

(8) Withdraw from consideration under the contract any employee receiving an unfavorable adjudication determination.

(9) Officially notify each contractor employee if he or she will no longer work on a Department contract.


(e) Further information including definitions of terms used in this clause and a list of required investigative forms for each risk designation are contained in Departmental Directive OM:5–101, “Contractor Employee Personnel Security Screenings” available at the Web site listed in the first paragraph of this clause.

(f) Failure to comply with the contractor personnel security requirements may result in a termination of the contract for default.

(End of clause)

3452.239-73 Federal desktop core configuration (FDCC) compatibility.

As prescribed in 3439.703, insert the following clause in all solicitations and contracts where software will be developed, maintained, or operated on any system using the FDCC configuration:

FEDERAL DESKTOP CORE CONFIGURATION (FDCC) COMPATIBILITY (MAR 2011)

(a) (1) The provider of information technology shall certify applications are fully functional and operate correctly as intended on systems using the Federal desktop core configuration (FDCC). This includes Internet Explorer 7 configured to operate on Windows XP and Windows Vista (in Protected Mode on Vista).


(b) The standard installation, operation, maintenance, update, or patching of software shall not alter the configuration settings from the approved FDCC configuration. The information technology should also use the Windows Installer Service for installation to the default “program files” directory and should be able to silently install and uninstall.

(c) Applications designed for normal end users shall run in the standard user context without elevated system administration privileges.

(End of clause)

3452.242–70 Litigation and claims.

As prescribed in 3442.7001, insert the following clause in all solicitations and resultant cost-reimbursement contracts:

170