UNITED STATES DEPARTMENT OF EDUCATION

OFFICE OF THE CHIEF FINANCIAL OFFICER

August 9, 2016

ACQUISITION ALERT 2016-07

TO: Contracting Officers and Contract Specialists

FROM: Senior Procurement Executive and Director, Enterprise Procurement Initiatives

SUBJECT: Class Deviation to Implement Policy Regarding Access to Contractor Information Systems

1. **Purpose:** The purpose of this alert is to issue a class deviation that allows Contracting Officers to require contractors and subcontractors at all tiers to afford the Department, other Federal agencies, the Comptroller General of the United States, and their authorized third-party representatives, full and timely access to contractor information systems and related resources to perform privacy and information security inspections.

2. **Deviated language:** FAR Part 39–Acquisition of Information Technology; FAR Part 12–Acquisition of Commercial Items

3. **Applicability:** This deviation applies to all solicitations and contracts for information technology which require security of information technology, and/or are for the design, development, or operation of a system of records using commercial information technology or support services.

4. **Effective Date:** August 9, 2016

5. **Expiration Date:** Effective until incorporated in the FAR, EDAR, or otherwise rescinded.

6. **Guidance:**
    a. *New Policy*: ED must ensure full and timely access to information systems and related resources of contractors and subcontractors at any tier to the extent required to perform privacy and information security inspections. ED will notify contractors and prospective contractors prior to award or during performance of the need for such access, and to incorporate into solicitations and contracts provisions requiring contractors to provide access to information systems and related resources, including information systems and related resources of subcontractors at any tier, to the extent required to conduct such inspections.
    b. *New Procedures*: Contracting Officers shall insert the clause in Attachment B in all solicitation and contracts for information technology (including acquisition of services that require the use of information technology to a significant extent) which require security of information technology, and/or are for the design, development, or operation of a system of records using commercial information technology services or support services. The incorporation of the clause in Attachment B in a solicitation or contract does not necessarily mean the Department has determined the acquisition to be an acquisition of information technology subject to any of the policies and procedures of FAR Part 39.

Contracting Officers should work in collaboration with the Department's Chief Information Security Officer (CISO), the Chief Privacy Officer (CPO), the Director of the Family Policy Compliance Office (FPCO Director), and other Department officials to determine whether an acquisition requires incorporation of the clause in Attachment B**. Absent a determination to the contrary, the clause in Exhibit A applies to solicitations and contracts that incorporate the clause at FAR 52.239-1.** The Contracting Officer may determine to include in solicitations a provision requiring offerors to represent in their quotes or proposals that they are aware of the need to provide full access to their information systems and related resources, and to those of their subcontractors, without undue delay or additional compensation.

7. **Attachments**:
   A. Class Deviation signed by the Chief Acquisition Officer, dated August 9, 2016.
   B. Deviated language.

8. **Additional Information:**
   Questions or comments about this class deviation may be directed to Todd Anthony at 202-245-6387 or todd.anthony@ed.gov; or David Munford at 202-245-8185 or david.munford@ed.gov.

Attachment B: Access to Contractor and Subcontractor Information Systems and Related Resources in Carrying out Privacy and Information Security Inspections

New definition within FAR 2.1–Definitions.

Subpart 2.101 – Definitions (DEVIATION)

2.101 Definitions.

Insert the following definitions in alphabetical order with existing 2.101 definitions:

Cloud computing means a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This includes other commercial terms, such as on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. It also includes commercial offerings for software-as-a-service, infrastructure-as-a-service, and platform-as-a-service.

Controlled unclassified information (CUI) means information that laws, regulations, or Government-wide policies require to have safeguard or dissemination controls, excluding classified information. Examples of CUI include but are not limited to Personally Identifiable Information (PII), Sensitive Personally Identifiable Information (SPII), and For Official Use Only (FOUO) information.

Government data means any information, document, media, or machine readable material regardless of physical form or characteristics, that is created or obtained by the Government in the course of official Government business.

Government-related data means any information, document, media, or machine readable material regardless of physical form or characteristics that is created or obtained by a contractor through the storage, processing, or communication of Government data. It includes related logical files and their content, file metadata, and log files generated from system processing and user activity. It does not include contractor's business records e.g. financial records, legal records etc. or data such as operating procedures, software coding or algorithms that are not uniquely applied to the Government data.

New sub-paragraph within FAR Part 12—Acquisition of Commercial Items

Insert the following sub-paragraph immediately following 12.301(f)(1):

(2) The clause at 52.239-70 (Deviation) has been authorized for inclusion in acquisitions of commercial items. Refer to 39.70 (Deviation) for provisions related to the use of this clause.

New subpart within FAR Part 39–Acquisition of Information Technology

Insert the following subpart immediately after Subpart 39.2–Electronic and Information Technology:

Subpart 39.70 – Access to Contractor and Subcontractor Information Systems and Related Resources in Carry out Privacy and Information Security Inspections (DEVIATION)

39.701 Authority and policy.

(a) *Privacy and information security inspections*. As authorized by law, the Government conducts various types of inspections, audits, examinations, or reviews related to the protection of privacy or the safeguarding of information and information systems. Such inspections (collectively referred to here as "privacy and information security inspections") may be undertaken for various purposes, including but not limited to:

(1) Examination of the security of federal information systems or of contractor information systems that process, store or transmit Government data, Government-related data, or controlled unclassified information, or which provide security protection for such systems (including vulnerability testing);

(2) Information Technology security reviews;

(3) Investigation and audit of administrative, technical, and physical safeguards taken to protect against threats and hazards to the integrity, confidentiality, and availability of Government data, Government-related data, or controlled unclassified information, or to the function of computer systems operated on behalf of the Government;

(4) Review of contractor policies, procedures and practices for handling Government data, Government-related data, controlled unclassified information and other sensitive data;

(5) Investigation of incidents involving actual or suspected improper releases of information (including cyber security incident response and reporting);

(6) Conduct of forensic analyses, investigation of computer crime, or the preservation of evidence of computer crime; and

(7) Review of the contractor's performance for compliance with the terms and conditions in the contract governing privacy and the security of information and information systems.

Such privacy and information security inspections are conducted in accordance with various statutes and regulations, executive orders, and government-wide guidance.

(b) *Policy*. It is the Government's policy to ensure the Government has full and timely access to information systems and related resources of contractors and subcontractors at any tier to the extent required to perform privacy and information security inspections. It is the Government's policy to notify contractors and prospective contractors prior to award or during performance of the need for such access, and to incorporate into solicitations and contracts provisions requiring contractors to provide access to information systems and related resources, including information systems and related resources of subcontractors at any tier, to the extent required to conduct such inspections.

39.702 Required access to information systems and related resources.

(a) *General requirement*. In acquisitions covered by this subpart, contractors and subcontractors at all tiers shall be required to afford the Government, any Federal agency and its subcomponents including the Office of Inspector General, the Comptroller General of the United States, and their authorized third-party representatives, full and timely access to contractor information systems and related resources to the extent required to carry out privacy and information security inspections. Acquisitions covered by this regulation are those Government acquisitions for information technology (including acquisition of services that require the use of information technology to a significant extent) which require security of information technology, and/or are for the design, development, or operation of a system of records using commercial information

technology services or support services. This requirement applies to commercial item acquisitions, including those for cloud-based computer services.

(b) *Subcontractor information systems and related resources*. The requirement for access to information systems and related resources applies to every subcontractor at any tier who is providing information technology (including services that require the use of information technology to a significant extent) which requires security of information technology, and/or is designing, developing, or operating a system of records using commercial information technology services or support services. The fact that some information or information system is owned by or is under the control of a subcontractor shall not excuse the prime contractor from ensuring full and timely access to the Government as necessary to conduct privacy and information security inspections. The contractor shall ensure that it retains operational and configurational control over any information system operated on behalf of the Government or which handles controlled unclassified information, Government data, or Government-related data (whether owned or operated by the contractor or a subcontractor) as needed to conduct privacy and information security inspections. Contractors subject to this requirement are required to flow down the requirement to all such subcontracts, including subcontracts for commercial items.

39.703 Procedures.

Source selection. In determining whether an acquisition is covered by this subpart, the Contracting Officer may collaborate with the Federal Agency's Chief Information Security Officer (CISO), the Chief Privacy Officer (the "CPO"), the Director of the Family Policy Compliance Office (the "FPCO Director"), and other Government officials. Absent a determination to the contrary, the clause at 52.239-70 (DEVIATION) applies to solicitations and contracts that incorporate the clause at 52.239-1.

39.704 Solicitation provisions and contract clauses.

(a) The Contracting Officer must insert the clause at 52.239-70 (DEVIATION) (Access to contractor and subcontractor information systems and related resources in carrying out privacy and information security inspections) in all solicitations and contracts for information technology (including acquisition of services that require the use of information technology to a significant extent) which require security of information technology, and/or are for the design, development, or operation of a system of records using commercial information technology services or support services. The incorporation of the clause at 52.239-70 (DEVIATION) in a solicitation or contract does not necessarily mean the Government has determined the acquisition to be an acquisition of information technology subject to any of the policies and procedures of Part 39.

(b) The Contracting Officer may determine to include in solicitations a provision requiring offerors to represent in their quotes or proposals that they are aware of the need to provide full access to their information systems and related resources, and to those of their subcontractors, without undue delay or additional compensation. In that case, the Contracting Officer shall insert the clause at 52.239-70 (DEVIATION) (ALTERNATE I) in the solicitation.

New clause within FAR Part 52 – Solicitation Provisions and Contract Clauses.

Insert the following clause immediately after the clause at 52.239-1, Privacy or Security Safeguards:

52.239-70 Access to contractor and subcontractor information systems and related resources in carrying out privacy and information security inspections (DEVIATION)

As prescribed in 39.704 (Deviation), insert the following clause in solicitations and contracts:

ACCESS TO CONTRACTOR AND SUBCONTRACTOR INFORMATION SYSTEMS AND RELATED RESOURCES IN CARRYING OUT PRIVACY AND INFORMATION SECURITY INSPECTIONS (DEVIATION)

(a) *Privacy and security inspections*. In accordance with the terms of this contract and as authorized by law, the Government carries out a program of privacy and information security inspections. Such inspections may be undertaken for various purposes, including but not limited to:

(1) Examination of the security of federal information systems or of contractor information systems that process, store or transmit Government data, Government-related data, or controlled unclassified information, or which provide security protection for such systems (including vulnerability testing);
(2) Information Technology security reviews;
(3) Investigation and audit of administrative, technical, and physical safeguards taken to protect against threats and hazards to the integrity, confidentiality, and availability of Government data, Government-related data, or controlled unclassified information, or to the function of computer systems operated on behalf of the Government;
(4) Review of contractor policies, procedures and practices for handling Government data, Government-related data, controlled unclassified information and other sensitive data;
(5) Investigation of incidents involving actual or suspected improper releases of information (including cyber security incident response and reporting);
(6) Conduct of forensic analyses, investigation of computer crime, or the preservation of evidence of computer crime; or
(7) Review of the contractor's performance for compliance with the terms and conditions in the contract governing privacy and the security of information and information systems.

(b) *Requirement to provide access to information systems and related resources*. The contractor shall afford the Government, any Federal agency and its subcomponents including the Office of Inspector General, the Comptroller General of the United States, and their authorized third-party representatives, full and timely access to contractor information systems and related resources to the extent required to carry out privacy and information security inspections. The contractor resources to which Government inspectors shall have access shall include the contractor's installations, facilities, infrastructure, data centers, equipment (including but not limited to all servers, computing devices, and portable media), operations, documentation (whether in electronic, paper, or other forms) including full and complete certification and accreditation records, databases, and personnel used in the performance of this contract.

In the case of security audits, access shall be provided to all systems, components, network devices, virtualized devices, and the like, for the purposes of evaluating the security postures and controls implemented to prevent unauthorized access, modification, or destruction to Government data and systems. In addition, the contractor shall provide the Government the following information upon request:

(1) any or all user-ids;

(2) any or all system and/or database administrator passwords used for the operation and maintenance of the system or environment, and
(3) security credentials, encryption keys, security algorithms, and the like;

to the extent needed to allow unfettered access to conduct a security audit or other privacy or information security inspection specified by the Government. The contractor shall also provide the Government access to all user passwords and all password files to the extent necessary to validate the contractor's password policy. The contractor agrees to provide user ids and passwords regardless of whether the user is a Federal employee or not, so long as the user works in support of a Government contract, or may have access to Government data or Government-related data.

In addition to providing such access, the contractor agrees to fully cooperate with the Government in its conduct of privacy and information security inspections. That cooperation shall include, among other things, timely and complete production of data, metadata, information, and records, and making employees of the contractor available for interview upon request. Cooperation also includes allowing the Government to make reproductions or copies of information and equipment, including, if necessary, collecting a machine or system image capture.

What constitutes "timely" access for purposes of compliance with this clause will depend on the circumstances surrounding the inspection being performed, the urgency of the matter under inspection, the procedures governing the inspection, logistical considerations, and other factors. In some cases, such as when investigating an on-going cyber security breach, access may be required within minutes of the Government's request. In other cases, access provided by the contractor within a few days of a request may be acceptable. In the event of an information security incident, including, but not limited to, incidents involving the loss or potential loss of Personally Identifiable information in physical or electronic form, the contractor must respond (as required by other provisions of this contract, Departmental Directive OM: 6-107 "External Breach Notification Policy and Plan" and Handbook OCIO-14 "Handbook for Information Security Incident Response and Reporting Procedures" within specified time frames. Access to the contractor and subcontractor's information systems under this clause shall be provided when, and as necessary, to meet any applicable information security incident response times.

(c) *Access to subcontractor information systems and related resources and clause flow-down*. Access shall also be provided to information systems and related resources of subcontractors at any tier that are providing information technology which requires security of information technology, and/or is designing, developing, or operating a system of records using commercial information technology services or support services. The fact that an information system is owned or operated by a subcontractor shall not excuse the prime contractor from ensuring full and timely access to such information systems and related resources to the extent necessary to conduct privacy and information security inspections under this contract or as authorized by law. The contractor shall ensure that it retains operational and configurational control over any information system (whether operated by the contractor or a subcontractor) as needed to conduct privacy and information security inspections.

The Contractor shall include the substance of this clause, including this paragraph (c), in all subcontracts, including subcontracts for commercial items.

(d) *Cost of compliance*. The aforementioned access and cooperation shall be provided by the contractor at no additional cost to the Government. However, if a Government inspection unduly

delays the contractor's performance of the contract, the Contracting Officer may grant a contractor's request for a non-compensable delay, as appropriate and provided the contractor submits information adequate to support the request.

(e) *Access to information systems where a cloud or a co-mingled data environment is used*. When the contractor will perform all or part of the work using commercial cloud computing services (whether directly or through a subcontract), or where Government data, Government-related data or controlled unclassified information will be comingled with non-Government data, the contractor shall ensure that appropriate measures and controls are in place to allow Government inspectors to search the information systems and access information needed to conduct required privacy and information security inspections. The contractor may choose to create (at no cost to the Government) a segregated data space where inspections may take place without undue interference with non-Government data. However, the fact that Government data and non-Government data is co-mingled in the contractor's information system shall not excuse the contractor from affording the Government full and timely access and cooperation as needed to conduct privacy and information security inspections.

The Government shall protect against the unauthorized use or release of information obtained from the Contractor (or derived from information obtained from the Contractor) under this clause that includes Contractor proprietary information. To the extent practicable, the Contractor shall identify and mark proprietary information. In making an authorized release of such information, the Government will implement appropriate procedures to minimize the Contractor proprietary information that is included in such authorized release, seeking to include only that information that is necessary for the authorized purpose(s) for which the information is being released

(f) *Miscellaneous*. The access obligations under this clause will survive the expiration or termination of this contract, and this term is not to be less than 3 years following the final disposition and close out of the contract.

(g) *Remedies for breach*. A breach of the obligations or restrictions set forth in this clause may subject the Contractor to a Termination for Default, in addition to any other appropriate remedies under the contract.

(h) *Relation to other requirements*. The requirements of this clause are in addition to those required by any other inspection or audit clause of this contract. To the extent that requirements imposed by Federal law, regulation, Executive Orders, Office of Management and Budget (OMB) guidance, or standards promulgated by the National Institute of Standards and Technology (NIST) are in direct and irreconcilable conflict with the requirements of this clause, those other requirements, standards, laws, or regulations shall take precedence.

In conducting its security testing the Government intends to follow *NIST Special Publication 800-115 Technical Guide to Information Security Testing and Assessment* and other appropriate testing and assessment standards. Further, the Contractor agrees to negotiate in good faith rules of engagement and other supplementary agreements to govern specific privacy and information security inspections, with the goal of ensuring access necessary to conduct such inspections while protecting the contractor's property and other interests. Any such rules of engagement and supplementary agreements are incorporated into this contract to the extent not inconsistent with the terms of this clause.

(End of Clause)

Alternate I (Deviation). As prescribed in 39.704(b) (Deviation), insert following paragraph (i) after paragraphs (a) to (h) of the basic clause:

(i) ____[insert name of offeror]_____hereby represents to the Government that it is aware of the requirement to provide full access to its information systems and related resources, and to those of its subcontractors (as set forth in paragraphs (a) to (h) above), without undue delay or additional compensation.