OFFICE OF THE UNDER SECRETARY OF DEFENSE
3000 DEFENSE PENTAGON
WASHINGTON, DC 20301-3000

ACQUISITION,
TECHNOLOGY
AND LOGISTICS

FEB 0 9 2015

In reply refer to
DARS Tracking Number: 2015-O0011

MEMORANDUM FOR COMMANDER, UNITED STATES SPECIAL OPERATIONS COMMAND (ATTN: ACQUISITION EXECUTIVE)
COMMANDER, UNITED STATES TRANSPORTATION COMMAND (ATTN: ACQUISITION EXECUTIVE)
DEPUTY ASSISTANT SECRETARY OF THE ARMY (PROCUREMENT)
DEPUTY ASSISTANT SECRETARY OF THE NAVY (ACQUISITION AND PROCUREMENT)
DEPUTY ASSISTANT SECRETARY OF THE AIR FORCE (CONTRACTING)
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Class Deviation—Contracting for Cloud Services.

Effective immediately, contracting officers shall follow the attached requirements (DFARS subpart 239.99, Cloud Computing (DEVIATION 2015-O0011)) and use the attached clause (DFARS 252.239-7999, Cloud Computing Services (DEVIATION 2015-O0011) (FEB 2015)) in contracts, task orders, and delivery orders in acquisitions for, or that may involve, cloud computing services.

The substance of this class deviation is addressed in DFARS Case 2013-D018, Network Penetration Reporting and Contracting for Cloud Services. Until the DFARS revisions contained in that case become effective, the information collection requirements (e.g., section 6.4 of the Cloud Computing Security Requirements Guide (SRG) referenced at 239.9902-1(c)(1)) of the attached deviation are not enforceable by the Government.

The deviation requires that the contracting officer, in conjunction with the requiring activity, ensure that any selected cloud computing solution is configured, deployed, and managed to meet the security, privacy, and other requirements of the organization, including applicable elements of the Federal Information Security Management Act of 2002 (FISMA) and the associated NIST standards and special publications (e.g., FIPS 199, FIPS 200, SP 800-53).

This class deviation remains in effect until incorporated in the DFARS or otherwise rescinded. My point of contact is Mr. Dustin Pitsch, who may be reached at 571-372-6090, or at Dustin.N.Pitsch.civ@mail.mil.

Richard Ginman
Director, Defense Procurement
and Acquisition Policy

Attachment:
As stated

[SUBPART 239.99—CLOUD COMPUTING (DEVIATION 2015-O0011)

239.9900 Scope of subpart. (DEVIATION 2015-O0011)

Prescribes policies and procedures for the acquisition of cloud computing services.

239.9901 Definitions. (DEVIATION 2015-O0011)

"Access," "cloud computing," "Government data," "Government-related data," and "spillage," as used in this subpart, are defined in the clause at 252.239-7999, Cloud Computing Services. (DEVIATION 2015-O0011)

239.9902 Policy and responsibilities. (DEVIATION 2015-O0011)

239.9902-1 General. (DEVIATION 2015-O0011)

(a) To the maximum extent practicable, cloud computing services that are commercial items shall be acquired under the terms and conditions (e.g., license agreements, End User License Agreements (EULA), Terms of Service (TOS), or other similar legal instruments or agreements) customarily provided to the public, to the extent that such terms and conditions are consistent with Federal law and otherwise satisfy the Government's needs, including those requirements specified in this section. Any applicable service provider terms and conditions shall be incorporated into the contract (e.g., by attachment or other appropriate mechanism).

(b) The contracting officer shall not award a contract to acquire cloud computing services from any cloud service provider (e.g., contractor or subcontractor, regardless of tier) that has not been granted provisional authorization to provide the relevant cloud computing services in accordance with the Cloud Computing Security Requirements Guide (SRG) (version in effect at time of contract award) found at http://iase.disa.mil/cloud_security/Pages/index.aspx. All necessary SRG requirements, including cloud access point connections and authorizations to operate, must be satisfied before the cloud computing service becomes operational.

(c) When contracting for cloud computing services, all purchase requests shall contain—

(1) A requirement to adopt and maintain administrative, technical, and physical safeguards and controls associated with the security level and services being provided, in accordance with the Cloud Computing Security Requirements Guide (SRG) (version in effect at time of award) found at

http://iase.disa.mil/cloud_security/Pages/index.aspx. Although the new cyber incident reporting requirements being established at SRG section 6.4 are not enforceable by the Government until the effective date of the information collection governing the new reporting requirements (i.e., in conjunction with the effective date of the corresponding reporting requirements contained in DFARS Case 2013-D018, Network Penetration Reporting and Contracting for Cloud Services), this does not limit or otherwise affect in any way the availability or enforceability of any other approved reporting requirements that are otherwise applicable and appropriately incorporated into the contract (e.g., reporting related to unclassified controlled technical information, or personally identifiable information);

(2) Government data and Government-related data descriptions;

(3) Data ownership, licensing, delivery, and disposition instructions specific to the relevant types of Government data and Government-related data (e.g., CDRL, SOW task, line item);

(4) Applicable privacy impact assessments requirements;

(5) Any additional information assurance requirements specific to the relevant types of Government data and Government-related data;

(6) Appropriate limitations and requirements regarding contractor and third party access to, and use and disclosure of, Government data and Government-related data;

(7) Appropriate requirements to support applicable inspection, audit, investigation, or other similar authorized activities specific to the relevant types of Government data and Government-related data, or specific to the type of cloud computing service being acquired; and

(8) A requirement to coordinate with the responsible Government official designated by the contracting officer to respond to any spillage occurring in connection with the cloud services being provided.

239.9903 Contract clauses. (DEVIATION 2015-O0011)

Use the clause at 252.239-7999, Cloud Computing Services, in solicitations and contracts for, or that may involve, cloud computing services.

*****

PART 252—SOLICITATION PROVISIONS AND CONTRACT CLAUSES

* * * * *

[252.239-7999 Cloud Computing Services. (DEVIATION 2015-O0011)
As prescribed in 239.9903, use the following clause:

CLOUD COMPUTING SERVICES (DEVIATION 2015-O0011) (JAN 2015)

(a) ***Definitions. As used in this clause—***

"Access" means the ability or opportunity to gain knowledge of Government or Government-related data or any other data collected or maintained on behalf of the United States Government under this contract.

"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.

"Government data" means any information, document, media, or machine readable material, regardless of physical form or characteristics, that is created or obtained 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. This does not include a contractor's business records, e.g., financial records, legal records, or data such as operating procedures, software coding or algorithms that are not uniquely applied to the Government data.

"Spillage" means an unauthorized transfer of classified data or controlled unclassified information to an information system that is not accredited for the applicable security level of the data or information.

(b) ***Cloud security requirements.*** **The Contractor shall adopt and maintain administrative, technical, and physical safeguards and controls that are required for the security level and services being provided, in accordance with the Cloud Computing Security Requirements Guide (SRG) (version in effect at the time of contract award) found at http://iase.disa.mil/cloud_security/Pages/index.aspx (Note: the new cyber incident reporting requirements of SRG section 6.4 become enforceable by the Government upon the effective date of the information collection governing the new reporting requirements (see DFARS case 2013-D018). However, this does not abrogate, limit, or otherwise affect the Contractor's obligation to comply with any other cyber incident reporting or other reporting requirement that is contained in this contract).**

(c) ***Limitations on access to, and use and disclosure of, government data and Government-related data.***

(1) The Contractor shall not access, use, or disclose Government data unless specifically authorized by the terms of this contract or a task order issued hereunder.

(i) If authorized by the terms of this contract or a task order issued hereunder, any access to, or use or disclosure of, Government data shall only be for purposes specified in this contract or task order.

(ii) The Contractor shall ensure that its employees are subject to all such access, use, and disclosure prohibitions and obligations.

(iii) These access, use, and disclosure prohibitions and obligations shall survive the expiration or termination of this contract.

(2) The Contractor shall use Government-related data only to manage the operational environment that supports the government data and for no other purpose unless otherwise permitted with the prior written approval of the Contracting Officer.

(d) ***Records management.***

(1) The Contractor shall deliver to the Contracting Officer all Government data and Government-related data in the format specified in the schedule.

(2) The Contractor shall dispose of Government data and Government-related data in accordance with the terms of the contract and provide the confirmation of disposition to the Contracting Officer in accordance with contract closeout procedures.

(e) ***Notification of third party access to Government data.*** **The Contractor shall notify the Government immediately of any requests from a third party for access to Government data or Government-related data, including any warrants, seizures, or subpoenas it receives, including those from another Federal, State, or Local agency, that could result in the disclosure of any Government data to a third party. The Contractor shall cooperate with the Government to take all measures to protect Government data from any loss or unauthorized disclosure that might reasonably result from the execution of any such request, warrant, seizure, subpoena, or similar legal process.**

(f) ***Spillage.*** **Upon written notification by the Government of a spillage, or the Contractor's discovery of a spillage, the Contractor shall coordinate immediately with the responsible Government official to correct the spillage in compliance with agency-specific instructions.**

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

(End of clause)