



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

SEP 19 2018

In reply refer to
DARS Tracking Number: 2018-O0020

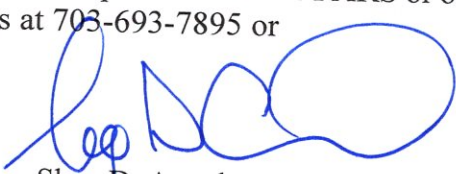
MEMORANDUM FOR COMMANDER, UNITED STATES SPECIAL OPERATIONS
COMMAND (ATTN: ACQUISITION EXECUTIVE)
COMMANDER, UNITED STATES TRANSPORTATION
COMMAND (ATTN: ACQUISITION EXECUTIVE)
COMMANDER, UNITED STATES CYBER
COMMAND (ATTN: ACQUISITION EXECUTIVE)
INSPECTOR GENERAL OF THE DEPARTMENT OF
DEFENSE
DEPUTY ASSISTANT SECRETARY OF THE ARMY
(PROCUREMENT), ASA (ALT)
DEPUTY ASSISTANT SECRETARY OF THE NAVY
(ACQUISITION & LOGISTICS MANAGEMENT),
ASN (RDA)
DEPUTY ASSISTANT SECRETARY OF THE AIR FORCE
(CONTRACTING), SAF/AQC
DIRECTORS, DEFENSE AGENCIES
DIRECTORS, DEFENSE FIELD ACTIVITIES

SUBJECT: Class Deviation—Permanent Supply Chain Risk Management Authority

Effective immediately, this class deviation removes the sunset date at DFARS 239.7300(b) and changes the statutory citations in DFARS subpart 239.73 from section 806 Pub. L. 111-383 to 10 U.S.C. 2339a. Contracting officers shall use the provision and clause provided in the attachment to this deviation in lieu of the provision at DFARS 252.239-7017, Notice of Supply Chain Risk, and clause at DFARS 252.239-7018, Supply Chain Risk, as prescribed in the attachment.

This class deviation implements section 881 of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2019 (Pub. L. 115-232). Section 881 codifies the authority for requirements for information relating to supply chain risk at 10 U.S.C. 2339a and repeals the sunset date at section 806(g) of the NDAA for FY 2011 (Pub. L. 111-383), as modified by section 806(a) of the NDAA for FY 2013 (Pub. L. 112-239), to make the authority permanent.

This class deviation remains in effect until incorporated in the DFARS or otherwise rescinded. My point of contact is Mary Thomas at 703-693-7895 or mary.s.thomas.civ@mail.mil.



Shay D. Assad
Principal Director, Defense Pricing
and Contracting

Attachment:
As stated

239.7300 Scope of subpart (DEVIATION 2018-O0020).

(a) This subpart implements 10 U.S.C. 2339a and elements of DoD Instruction 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN), at (<http://www.dtic.mil/whs/directives/corres/pdf/520044p.pdf>).

(b) The authority provided in this subpart is permanent (see 10 U.S.C. 2339a).

239.7301 Definitions (DEVIATION 2018-O0020).

As used in this subpart—

“Covered item of supply” means an item of information technology that is purchased for inclusion in a covered system, and the loss of integrity of which could result in a supply chain risk for a covered system (see 10 U.S.C. 2339a).

“Covered system” means a national security system, as that term is defined at 44 U.S.C. 3552(b) (see 10 U.S.C. 2339a). It is any information system, including any telecommunications system, used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—

- (1) The function, operation, or use of which—
 - (i) Involves intelligence activities;
 - (ii) Involves cryptologic activities related to national security;
 - (iii) Involves command and control of military forces;
 - (iv) Involves equipment that is an integral part of a weapon or weapons system; or
 - (v) Is critical to the direct fulfillment of military or intelligence missions, but this does not include a system that is to be used for routine administrative and business applications, including payroll, finance, logistics, and personnel management applications; or
- (2) Is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

* * * * *

“Supply chain risk” means the risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a covered system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system (see 10 U.S.C. 2339a).

* * * * *

252.239-7017 Notice of Supply Chain Risk (DEVIATION 2018-O0020).

Use the following provision, in lieu of the provision at DFARS 252.239-7017, in all solicitations, including solicitations using FAR part 12 procedures for the acquisition of commercial items, for information technology, whether acquired as a service or as a supply, that is a covered system, is a part of a covered system, or is in support of a covered system, as defined at 239.7301 (DEVIATION 2018-O0020):

NOTICE OF SUPPLY CHAIN RISK (SEP 2018) (DEVIATION 2018-O0020)

(a) *Definition.* As used in this provision—

“Supply chain risk,” means the risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a covered system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system (see 10 U.S.C. 2339a).

(b) In order to manage supply chain risk, the Government may use the authorities provided by 10 U.S.C. 2339a. In exercising these authorities, the Government may consider information, public and non-public, including all-source intelligence, relating to an offeror and its supply chain.

(c) If the Government exercises the authority provided in 10 U.S.C. 2339a to limit disclosure of information, no action undertaken by the Government under such authority shall be subject to review in a bid protest before the Government Accountability Office or in any Federal court.

(End of provision)

252.239-7018 Supply Chain Risk (DEVIATION 2018-O0020).

Use the following clause, in lieu of the clause at DFARS 252.239-7018, in all solicitations and contracts, including solicitations and contracts using FAR part 12 procedures for the acquisition of commercial items, for information technology, whether acquired as a service or as a supply, that is a covered system, is a part of a covered system, or is in support of a covered system, as defined at 239.7301 (DEVIATION 2018-O0020):

SUPPLY CHAIN RISK (SEP 2018) (DEVIATION 2018-O0020)

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

“Information technology” (see 40 U.S.C 11101(6)) means, in lieu of the definition at FAR 2.1, any equipment, or interconnected system(s) or subsystem(s) of equipment, that is used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency.

(1) For purposes of this definition, equipment is used by an agency if the equipment is used by the agency directly or is used by a contractor under a contract with the agency that requires—

(i) Its use; or

(ii) To a significant extent, its use in the performance of a service or the furnishing of a product.

(2) The term “information technology” includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources.

(3) The term “information technology” does not include any equipment acquired by a contractor incidental to a contract.

“Supply chain risk,” means the risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a covered system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system (see 10 U.S.C. 2339a).

(b) The Contractor shall mitigate supply chain risk in the provision of supplies and services to the Government.

(c) In order to manage supply chain risk, the Government may use the authorities provided by 10 U.S.C. 2339a. In exercising these authorities, the Government may consider information, public and non-public, including all-source intelligence, relating to a Contractor’s supply chain.

(d) If the Government exercises the authority provided in 10 U.S.C. 2339a to limit disclosure of information, no action undertaken by the Government under such authority shall be subject to review in a bid protest before the Government Accountability Office or in any Federal court.

(End of clause)